日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　６月２３日
出願番号 Application Number: [ST. 10/C]:	特願２００３－１７７４５６ [ＪＰ２００３－１７７４５６]
出願人 Applicant(s):	株式会社日立製作所

U.S. Appln. Filed 2-27-04
Inventor: T. Miyata et al
Mattingly Stanger & Malur
Docket HIT-415

２００４年　２月２０日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０１１７５０

【書類名】　特許願
【整理番号】　H03007821A
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
　【氏名】　宮田　辰彦
【発明者】
　【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
　【氏名】　川井　恵理
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100075096
　【弁理士】
　【氏名又は名称】　作田　康夫
　【電話番号】　03-3212-1111
【手数料の表示】
　【予納台帳番号】　013088
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報公開設定制御方法、情報管理装置および該情報管理装置を用いたサービス

【特許請求の範囲】

【請求項１】

登録されたユーザの種々の属性情報（オブジェクト情報）の、他者に対する開示可否（パーミッション）の設定値を、該開示可否のレベルに応じて分類し、階層的に管理するサーバ。

【請求項２】

請求項１に記載のサーバにおいて、前記パーミッションの設定値を、当該オブジェクト情報に対する公開の可否、当該オブジェクト情報に対する読出し（read）可否、当該オブジェクト情報に対する書き込み（write）可否の３種のレベルに分類して管理することを特徴とするサーバ。

【請求項３】

請求項２に記載のサーバにおいて、

前記公開の可否は、前記読出し可否に対する上位のパーミッションレベルとして設定され、

前記読み出し可否は、前記書き込み可否に対する上位のパーミッションレベルとして設定され、

当該パーミッションレベルの上位・下位の関係を基準として、所定のパーミッションの設定値の矛盾を検出することを特徴とするサーバ。

【請求項４】

請求項２に記載のサーバにおいて、あるオブジェクト情報に対するあるパーミッションレベルのうち、前記公開可否以外のパーミッションレベルに対して、設定値の変更要求がユーザからあった場合、

当該変更要求があったレベルの上位に属する全てのレベルのパーミッション設定値の、当該変更要求のあった設定値に対する整合性をチェックすることを特徴とするサーバ。

【請求項５】

請求項４に記載のサーバにおいて、

前記整合性に矛盾があった場合、当該設定値の変更要求のあったレベルのパーミッションの上位に属するレベルのパーミッション設定値を修正することを特徴とするサーバ。

【請求項６】

請求項４に記載のサーバにおいて、

前記オブジェクト情報に対し、当該オブジェクト情報の種類に応じた上位・下位の関係を付与し、系統的に分類して管理することを特徴とするサーバ。

【請求項７】

請求項６に記載のサーバにおいて、あるオブジェクト情報に対する任意のレベルのパーミッション設定値に対し、当該設定値の変更要求がユーザからあった場合、

該変更要求を受けた設定値の属するオブジェクト情報の上位のオブジェクト情報に含まれるパーミッション設定値の、当該変更要求を受けた設定値に対する整合性をチェックすることを特徴とするサーバ。

【請求項８】

請求項７に記載のサーバにおいて、前記整合性に矛盾があった場合、前記変更要求を受けた設定値が属するオブジェクト情報の上位に属するオブジェクト情報に属するパーミッション設定値を修正することを特徴とするサーバ。

【請求項９】

請求項１に記載のサーバにおいて、前記属性情報に対し、当該属性情報の種類に応じた上位・下位の関係を付与し、系統的に分類して管理することを特徴とするサーバ。

【請求項１０】

送信された情報を受信するインターフェースと、記憶手段と、該記憶手段に格納された情報を読み出す手段とを有し、

前記記憶手段は、登録されたユーザの種々の属性情報（オブジェクト情報）と、開示レベルに応じて分類された前記属性情報の他者に対する開示可否（パーミッション）の設定値とが記録されたエントリテーブルを備えることを特徴とする

サーバ。

【請求項１１】

請求項１０に記載のサーバにおいて、前記パーミッションの設定値は、相互に上位・下位の関係付けがされた複数のレベルに分類され、

前記エントリテーブルには、該複数のレベルのいずれかに対して付与された設定値が記録されていることを特徴とするサーバ。

【請求項１２】

請求項１１に記載のサーバにおいて、

前記パーミッションの設定値は、前記オブジェクト情報に対する公開の可否、当該オブジェクト情報に対する読出し（read）可否、当該オブジェクト情報に対する書き込み（write）可否の３つのレベルに分類され、

前記エントリテーブルには、前記３つのレベルのいずれかに対して付与された設定値が記録されていることを特徴とするサーバ。

【請求項１３】

請求項１１に記載のサーバにおいて、

受信した情報からパーミッションの設定値の変更要求を抽出する手段と、

前記エントリテーブルを参照し、前記変更要求のあったパーミッションの設定値が、当該設定値の上位のパーミッションの設定値と矛盾しないかどうかを判定する判定手段とを備えることを特徴とするサーバ。

【請求項１４】

請求項１２に記載のサーバにおいて、

前記変更要求のあった設定値と、当該設定値の上位のパーミッション設定値とに矛盾があった場合、該上位のパーミッション設定値を修正する手段を有することを特徴とするサーバ。

【請求項１５】

請求項１１に記載のサーバにおいて、前記エントリテーブルのコピーデータが格納された外部記憶装置を備えたことを特徴とするサーバ。

【請求項１６】

登録されたユーザの種々の属性情報（オブジェクト情報）の他者に対する開示

可否（パーミッション）の設定値に対し、該開示可否のレベルに応じて上位・下位の関係を付与して階層的に管理するサーバの制御方法。

【請求項１７】

請求項１６に記載のサーバの制御方法において、

前記登録されたユーザからの所定のオブジェクト情報に対するパーミッション設定値の変更要求を受信し、

該設定値がどのレベルのパーミッション設定値に対する変更要求かを判断し、

当該レベルの上位に属するパーミッションの設定値が前記変更要求されたパーミッション設定値と矛盾しないかを判断し、

矛盾がある場合は、前記レベルの上位に属するパーミッションの設定値を修正することを特徴とするサーバの制御方法。

【請求項１８】

請求項１６に記載のサーバの制御方法において、

前記オブジェクト情報に対し、当該オブジェクト情報の種類に応じた上位・下位の関係を付与し、分類して管理することを特徴とするサーバの制御方法。

【請求項１９】

請求項１８に記載のサーバの制御方法において、

前記登録されたユーザからの所定のオブジェクト情報に対するパーミッション設定値の変更要求を受信し、

該オブジェクト情報がどのレベルに属する情報かを判断し、

当該変更要求を受けたパーミッション設定値の属するオブジェクト情報の上位レベルに属するオブジェクト情報のパーミッション設定値と、当該変更要求されたパーミッション設定値とが矛盾しないかどうかを判断し、

矛盾する場合は、ユーザに設定変更拒否の通知を行なうことを特徴とするサーバの制御方法。

【請求項２０】

登録されたユーザの種々の属性情報（オブジェクト情報）の、他者に対する開示可否（パーミッション）の設定値を、該開示可否のレベルに応じて分類し、階層的に管理するプレゼンスサーバと、前記ユーザに対してサービスを提供するた

めのサービス提供サーバと、前記ユーザがサービス提供を受けるための端末とを有し、

前記サービス提供サーバは、前記プレゼンスサーバに対して、サービスを提供しようとしているユーザの所定のオブジェクト情報に対しアクセス要求を行ない、

前記プレゼンスサーバは、該アクセス要求のあったオブジェクト情報に対し、パーミッションの設定値の範囲内で与えることのできるオブジェクト情報を前記サービス提供サーバに対して送信し、

該サービス提供サーバは、受信したオブジェクト情報を元にユーザに対してサービスを提供することを特徴とするサービス提供システム。

【請求項２１】

登録されたユーザの種々の属性情報（オブジェクト情報）の、他者に対する開示可否（パーミッション）の設定値を、該開示可否のレベルに応じて分類し、階層的に管理するプレゼンスサーバと、前記ユーザに対してサービスを提供するためのサービス提供サーバと、前記ユーザがサービス提供を受けるための端末とを少なくとも含むシステムを用いたサービス提供方法であって、

前記サービス提供サーバは、前記プレゼンスサーバに対して、サービスを提供しようとしているユーザの所定のオブジェクト情報に対しアクセス要求を行ない、

前記プレゼンスサーバは、該アクセス要求のあったオブジェクト情報に対し、パーミッションの設定値の範囲内で与えることのできるオブジェクト情報を前記サービス提供サーバに対して送信し、

該サービス提供サーバは、受信したオブジェクト情報を元にユーザに対してサービスを提供することを特徴とするサービス提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報公開の設定方式に関する。

【０００２】

【従来の技術】

通信技術とネットワーク技術の発展に伴い、いつでもどこでもコミュニケーションを取れるユビキタスネットワーク社会が到来しつつある。ユビキタス社会でのコミュニケーションでは、各ユーザが自他者の個人情報をデータベースに登録し、種々のサービスを受けることが可能になるといわれている。

【０００３】

現在、データベース上でプライバシ保護を管理する方式の一つに、Unixシステム（Unixは登録商標）で用いられているパーミッションシステムがある。これはディレクトリ構造を持ったファイルシステム上のディレクトリないしファイルに対し、保有者、グループ、他人と3分割されたアクセス単位を用いて、アクセス単位ごとにRead（読み出し）、Write(書き込み)、Execute（実行）の3操作について、アクセス可否のパーミッションを設定する方式である。パーミッションの設定は、通常、システム全体の管理者により行われている。

【０００４】

図２７には、Unixシステムで用いられているファイルシステムの構造図に、パーミッション設定で用いられるパラメータを併せて示した。本図を用いて、Unixで行われているパーミッション管理方式について説明する。

【０００５】

まず、図２７の前提条件について説明する。図２７のファイルシステムは、rootディレクトリの下に、第１階層ディレクトリ、第２階層ディレクトリが複数個形成され、第２階層ディレクトリの下層にfile A, file B, file Cの３つのファイルが格納されたツリー構造を有している。本ファイルシステム上には、User A, User B, User Cの３ユーザが存在しているとする。また、User A, User CによりGroup Aが、User A, User B によりGroup Bが形成されているものとする。ファイルシステムの外側の各四角は、各ディレクトリ、各ファイルに対する、アクセス権限の所在と種別（以下、パーミッション）の設定値を示している。例えば、file Aの右側の四角はfile Aに対するパーミッションの設定値を示している。file Aに対するパーミッションの設定によれば、file AのオーナはUser Aであり、グループパーミッションが与えられたグループはGroup Aである。また、オー

ナに与えられたアクセス権限の種別は、r、w、xであり、すなわちRead、Write、Executeのいずれの操作も実行可能である。また、グループに与えられた権限はr、wであり、すなわち、Group Aに属するユーザが可能な操作はRead、Write操作である。他人に与えられた権限は－であり、他人は、file Aを全く操作できない。

【０００６】

図示されていないが、本ファイルシステムには、パーミッション管理を行なう管理機能を備えているものとする。パーミッションの各設定値は、Unixファイルシステムが格納されたストレージ内に保管されており、各ディレクトリやファイルへのアクセスが発生するたびに、ファイルシステムが当該記憶手段を参照してパーミッションを判定する。

【０００７】

次に、User A, User B, User Cが、file A, file B, file Cへアクセスする際のパーミッションの判定方法について説明する。

【０００８】

User Aがfile Aにアクセスを行う場合，rootディレクトリ，第１階層ディレクトリ，第２階層ディレクトリ，ファイルの順番にアクセスを開始する。実際にはhome, User A, file Aの順番でアクセスを行う。ファイルシステムのアクセス管理サーバは、まず、User Aがアクセスしようとするhome、User Aの各ディレクトリおよびfile Aのオーナが誰であるか確認する。オーナは全てUser Aであり、オーナに対しては、全ての階層で、r、w、xの各操作が許可されている。従って、User Aがfile Aに対してアクセスする場合、ファイルシステムは、User Aに対し、第１階層ディレクトリ、第２階層ディレクトリの順でアクセスを許可し、最終的にfile Aへのアクセスを許可する。次に、file Aに対して、write, read, 実行すべての処理の実行をも許可する。

【０００９】

一方、file B、file Cに対しては、User Aはオーナではない。そこでfile B、file CへのUser Aのアクセス判定に際しては、ファイルシステムは、グループパーミッションを確認する。例えば、User AはGroup Bに属している。file Bの右

側の四角内に示されたパーミッション設定値によれば、Group Bに属するユーザはfile Bに対してread，writeの操作を行える。従ってファイルシステムは、User Aに対しては、file Bへのread，write操作のみを許可する。file Cに対するパーミッションも同様である。

【００１０】

次にUser Bのファイルアクセスについて説明する。User Bがhomeにアクセスを行うと、ファイルシステムは、User Bのhomeへのアクセス権限について判定を行う。User B は、homeのオーナでもなく、Group Aに属してもいない。よって、ファイルシステムは他人に対するパーミッションを確認するが、他人に対するパーミッションの内容はすべて不許可に設定されている。従って、User Bはhomeに対してアクセス権限がなく、home以下のすべてのディレクトリ，ファイルにアクセスすることが出来ない。file Bのオーナは User Bであるが、上層でアクセスが塞がれているので、自分がオーナであるfile Bであってもアクセスが出来ない。

【００１１】

次にUser Cのファイルアクセスについて説明する。User CはGroup Aに属しているので， User Cは、home，User Aの各階層のディレクトリに対してアクセス権限を持っている。よって、ファイルシステムは、User Cが第２階層ディレクトリを通過するまでは許可する。file Aについては、User C はオーナではないので、グループパーミッションを確認する。User C はGroup Aに所属しているので、ファイルシステムは、User Cに対し、file A へのread，writeを許可する。file Bについては、User Cはオーナでも Group Bに所属してもいないので、ファイルシステムは他人に対するパーミッションを確認し，User Cのfile Bへのアクセスは許可しない。file Cについては、User Cがオーナであるから、ファイルシステムはwrite，read，実行の全操作を許可する。

【００１２】

このようにUnixのアクセス制御管理では上位のディレクトリを確認しながら下位のディレクトリ，ファイルにアクセス管理を行うので、上位のディレクトリにパーミッションが無い場合，下位にアクセスすることが出来なくなる。つまり，下位のパーミッションをいくら変更しても上位のパーミッションも同様に変更し

ない限りアクセスすることが出来ない。更にまた，新しいアクセスユーザ範囲を設定するときは新たにグループを作成してグループに対するパーミッション設定を行う必要がある。

【００１３】

また、他の方式にリレーショナルデータベースで用いられているようなアクセスコントロールがある。これは各アクセス者、あるいは何人かのアクセス者が集まったグループに毎に、データベースのレコードに対するアクセス権を設定する方式である。簡単にいえば、ツリー構造を用いないようなファイルシステムであって、リレーショナルデータベースの各データテーブルへのパーミッションをアクセス者毎に設定する。パーミッション設定は、データベースシステムの管理者が行う。

【００１４】

【発明が解決しようとする課題】

ユーザの個人情報に基づき種々のサービスを行うようなビジネスでは、ユーザの現在状況や時間帯、気分などにより、個人情報の開示可否の設定変更が頻繁に発生する。従来のパーミッション管理方式は、管理者が一度アクセスコントロールの設定を行った後は、設定変更頻度が多くないという前提の上に開発されており、頻度の高い更新に対して頻度を軽減するようなしくみがない。

【００１５】

また、従来技術では、パーミッションの管理システムはファイルやデータベースサーバに付随し、特定のデータ毎にパーミッション管理を行っていた。例えば、Unixのファイルシステムでは、ファイルとして管理される文書、画像等、種々のデータ毎にパーミッション管理を行っている。しかし、個人情報に基づきサービスを提供するビジネスの場合、サービス提供者の保有するサービス提供手段（サーバ等）は、ユーザが提供を受けようとするサービスの種類により物理的に異なる。例えば、デパートでの商品購入履歴はデパートが持つサーバに保存されるだろうし、端末の位置情報は端末の管理キャリアのサーバに保存される。各ユーザが自分の情報に対するパーミッションを変更したい時、これらサーバに個別にアクセスするのでは設定が煩雑であり、ユーザの負担が大きい。更に、サービス

提供者の保有するサーバについても、パーミッション設定を管理するデータベースを個別に持つ必要が出てくる。

【００１６】

更に、このようなパーミッション設定においては、開示する個人情報の機密のレベルに応じて、各個人情報間に上位・下位の関係が存在する。つまり、個人情報を、機密の度合いに応じて分類して管理する必要が出てくる。

【００１７】

更にまた、サービス提供者がユーザの個人情報を利用して第三者にサービスを提供するような場合、プライバシ保護の関係上、Read、Writeの可否だけを管理して第三者に対するユーザの個人情報へのアクセス可否を判断するだけでなく、情報の存在そのものを隠蔽する必要がある場合もある。従来技術では、アクセス対象となるデータの参照要求に合わせてパーミッションの可否を判断する管理方式であったため、存在そのものを隠蔽することができなかった。すなわち、パーミッション可否が判断された＝アクセス対象が存在する、であった。

本発明は、パーミッションに限らず、上下関係を持った情報群を適切に管理することが可能なサーバ、あるいは当該サーバを用いたサービスモデルを提供することを目的とする。

【００１８】

【課題を解決するための手段】

本特許出願は、２つの発明を含んでいる。

第１の本発明は、パーミッションの設定値を専門に管理する管理サーバを設けることであり、これより、サービス提供者毎にパーミッション設定を行う必要があるという、設定の煩雑さという課題を解決する。

【００１９】

第２の本発明は、パーミッション設定値のような上下関係をもった情報群を、上下関係に応じて複数に分類して管理することにより、パーミッション設定値を適切に管理する。あるいは、上下関係を識別可能な識別コードを情報群に与えて管理する。

更に、他のパーミッションに対して相対的に下位のパーミッションに対する設定

変更要求を受けた場合に、上位のパーミッションの設定値を自動変更することにより、パーミッションの上下関係の整合性を保つことを可能とする。

【００２０】

【発明の実施の形態】

以下の実施例では、個人情報、プレゼンス情報等を含むユーザの属性情報をオブジェクト情報と称し、第三者に対する個々のオブジェクト情報の開示可否をパーミッションと称する。

（実施例1）

本実施例では、プレゼンスサーバの構造、動作、及びプレゼンスサーバを用いたサービスを実現するためのネットワークについて説明する。

【００２１】

図１には、本実施例のプレゼンスサーバの機能ブロック図を模式的に示した。図１の機能ブロック図は、ソフトウェア上実現される論理的な機能構成を示した図であるが、各機能ブロックをハードウェアで構成しても構わない。

【００２２】

図２には、図１に示した機能ブロックが、ハードウェア上、どう実現されているかを示した。図１に示した種々の機能ブロックの動作は、ＣＰＵ21によって実行されている。個々の機能ブロックが動作する際に必要なパーミッションの設定値は、メモリ22に格納されており、ＣＰＵ21は、メモリ22に格納されたエントリテーブルを読み出すことにより、必要な情報を取り出す。

【００２３】

次に、プレゼンスサーバ1が、ユーザからのパーミッション設定要求を受信して、その内容を図２のパーミッション設定テーブル24に書き込むまでの全体的な動作について説明する。

ユーザが自分の情報に対するパーミッション設定要求を端末から送信すると、プレゼンスサーバ1の各インターフェース11－1～11－ｎがその送信メッセージを受信する。そこでそのメッセージはまず、パーミッション情報処理部2に転送され、パーミッション情報送受信部4がそのメッセージを受信する。次にメッセージをパーミッション情報抽出・転送部5に送信する。パーミッション情報抽出・転

送部5では、メッセージの中からパーミッション設定要求の部分を抽出して、サーバ内部で解釈できるデータ形式に変換を行い、変換されたユーザ設定要求をパーミッション管理部3に転送する。

【００２４】

パーミッション管理部3ではその要求をパーミッション設定内容整合部9が受信し、設定内容の整合を行い、整合したパーミッション設定をパーミッション設定内容入力部7に転送する。パーミッション設定内容入力部7は図２のデータバス27を介してメモリ22上にあるテーブル記憶部26に設定内容を転送、テーブル記憶部26はパーミッション設定テーブル24に設定内容を記憶する。記憶が終わると終わったことがパーミッション設定内容入力部7を介してパーミッション設定内容整合部9に送信されそれを受信すると、パーミッション設定が成功したことを示すメッセージをパーミッション情報送受信部4に送信してインターフェース11を介してそれをユーザに送信する。

【００２５】

次に、本実施例のプレゼンスサーバ1が、ユーザの要求により、プレゼンスサーバ1に記憶されたパーミッション情報を読み出してユーザに送信する時の全体的な動作について説明する。まずユーザからのパーミッション取得要求メッセージを受信したインターフェース11はそのメッセージをパーミッション情報送受信部4で受信する。パーミッション情報送受信部4はその情報をパーミッション出力内容計算部10に送信する。パーミッション出力内容計算部25はパーミッション設定内容出力部8と図２のデータバス27を介してテーブル呼び出し部25からパーミッション設定テーブル24にある要求されたパーミッション設定内容を呼び出す。その後、パーミッション出力内容計算部はその設定内容について矛盾が発生しないように計算を行い、その内容をパーミッション情報構築部6に転送する。パーミッション情報構築部6は受信したパーミッション設定内容をユーザクライアントが解釈できる形式に変換を行い、パーミッション情報送受信部を介してパーミッション設定内容を記述したメッセージをインターフェース11から送信する。管理コンソールは、プレゼンスサーバの管理者が種々の設定を行うための装置である。

【００２６】

図３には、オブジェクト情報を分類するための階層構造モデルを示す。本実施例において想定している階層モデルでは、ユーザＩＤ31は、階層モデルの最上位の情報に位置する。ユーザＩＤは、各ユーザを一意に識別可能なＩＤであれば何でも良く、数値やコードの替りに、氏名と住所などを組み合わせて使用することもできる。ユーザＩＤの１階層下位には、ユーザに付随する情報32が位置する。ユーザに付随する情報とは、例えば、各ユーザが携帯電話を所有しているか否か、特定のサービスに加入しているか否かなどを示す情報である。ユーザに特定のサービスを受ける意志があるかどうかを示す情報と言い換えても良い。ユーザは、複数の端末を所有している場合もあり得るし、全く所有していない場合もあり得る。サービスについても同様である。

【００２７】

ユーザの付随情報の１階層下位には、端末ＩＤ33-1～33-nやサービスＩＤ34-1～34-nが位置する。本モデルでは、端末ＩＤやサービスＩＤが判れば、端末種別やサービスの種別は自動的に判明するものと考えているが、端末種別情報やサービス種別情報を、各ＩＤ情報と別にし、更に１階層下位に位置づけても良い。端末ＩＤとしては、例えば、電話番号やＳＩＰ（Session Initiation Protocol）、ＵＲＩ等が使用できる。また、サービスＩＤとは、例えば、サービス提供業者がサービス加入者に対して割り振るＩＤである。いうまでもないが、端末種別情報とは、端末が例えば、PDA33-nであるか携帯電話33-1であるか、あるいはPCなどの固定端末であるか等を示す情報である。サービス種別情報とは、例えば、ユーザが加入しているサービスが、ＩＭサービス34-1～であるかビデオチャットサービス34-nであるかを示す情報である。

【００２８】

端末ＩＤ33-1～33-nおよびサービスＩＤ34-1～34-nのさらに1階層下位には、また各端末やサービスに付随する各種の情報35-1～35-n ～38-1～38-n が位置する。端末付随情報とは、例えば、端末毎に持つオンラインステータスや話中ステータス、位置情報等、各種端末に付随する各種の情報である。また、サービス付随情報とは、各サービス提供業者がサービスを展開するのに必要とする情報のこ

とであり、例えば、星占いのサービス提供業者であれば、サービス加入者の生年月日や星座などの情報が該当する。プレゼンスサーバ1は、種々のオブジェクト情報を、図３の階層モデルに従って記憶する。

【００２９】

図３では、4層の階層モデルを示したが、構造をもっと細分化して、より多層の構造としてオブジェクト情報を記憶しても良い。また、構造をもっと簡略化して、３層や２層の階層としてオブジェクト情報を記憶しても良い。実際には、２層目のユーザ付属情報は考慮しなくても良い場合が多い。端末を持っていないユーザや、サービスに加入していないユーザは、そもそもユーザＩＤを持たない場合が多いからである。ただし、ユーザやサービス提供者の都合によっては、付属情報32の階層を設けた方がよい場合があり得る。例えば、ユーザが、一時的にサービスの享受を停止して、しばらく経った後にサービス享受を再開したい場合や、サービス提供者の方から、ユーザへのサービス提供を一時的に中断したい場合など（例えば、ユーザが料金を支払えなくなった場合等）、以前のユーザＩＤがそのまま使用できて便利である。

【００３０】

図４は、各オブジェクト情報に対して設定されるパーミッションに上下関係があることを示した図である。プレゼンスサーバ1が持つパーミッション情報の階層構造はオブジェクト情報の階層構造と同様となる。図３と図４とを対比すると、図４の第１の階層構造が、図３のユーザＩＤ層に相当する。プレゼンスサーバ1は、ユーザＩＤに対するパーミッション41を最上位のパーミッションとして認識し、記憶する。その1階層下位にはユーザに付随する各情報に対するパーミッション42、各サービスＩＤに対するパーミッション43、各端末ＩＤに対するパーミッション44を、さらにその1階層下位にはサービスに付随する各情報へのパーミッション45、端末に付随する各情報に対するパーミッション46を記憶する。プレゼンスサーバ1はこの構造を持ったパーミッション設定情報を、オブジェクト情報の設定を行なったユーザとその情報を閲覧しようとする第三者（サービス提供業者のみならず、いわゆる第三者も含む）との組み合わせの数だけ記憶する。

【００３１】

図５は本願発明のプレゼンスサーバ1が取り扱うオブジェクト情報に対するパーミッション設定の設定種別単位での記憶構造を示した図である。パーミッションの設定値は、あるオブジェクト情報をどの程度第三者に対して開示したいかの度合いによって、複数の値を取りうる。本実施例では、各オブジェクト情報41～46に対して設定できるパーミッションの種別は、公開設定52、Read設定53、Write設定54の３種とした。52～54の各種別に対しては許可56、もしくは拒否57の値を設定できる。

【００３２】

公開設定52とは閲覧ユーザに対してその情報を見せるか、見せないかを決める設定であり、55－1のように許可と設定すると閲覧ユーザに情報を見せ、56－1のように拒否と設定すると閲覧ユーザに情報を見せないようにする。拒否設定をされた閲覧ユーザはその情報を公開ユーザが所有していることを知ることができなくなる。例えばユーザＩＤ41に対して公開設定52を拒否と設定すると閲覧ユーザは公開ユーザのユーザＩＤを知ることができない。つまりその公開ユーザの存在を第三者に対して隠蔽することができる。逆にいえば、オブジェクト情報の隠蔽機能をプレゼンスサーバに付加する場合は、パーミッションの設定種別に、公開設定というパラメータを設けなければならない。

【００３３】

Read設定53とは、閲覧ユーザに対するその情報の読み出しの許可、もしくは拒否を決める設定であり、55－2のように許可と設定すると閲覧ユーザはその情報を見ることが可能となり、56－2のように拒否と設定すると閲覧ユーザがその情報の閲覧を要求した時に、公開拒否されたことが通知される。

【００３４】

Write設定54とは閲覧ユーザに対するその情報の書き込みの許可、もしくは拒否を決める設定であり、55－3のように許可と設定すると閲覧ユーザがその情報の登録、もしくは更新を行うことが可能となる。つまり公開ユーザが所有する情報を第3者が代理で更新することが可能となる。各オブジェクト情報には1情報につきこの3つのパーミッション設定を行うことが可能である。また、この3つの設定は階層構造を取る。プレゼンスサーバは各オブジェクト情報41～46に対してま

ず最上位の設定を公開設定52とし、その下位をRead設定53、さらにその下位をWrite設定54としてパーミッション情報を取り扱う。また、これら3つの設定の内容については法則性がある。例えば、最下位のWrite設定54が許可の場合は上位のRead設定53も許可となり、さらに最上位の公開設定52も許可となる。また、最上位の公開設定52が拒否であれば下位のRead設定53、Write設定54も同様に拒否となる。つまり、上位設定が拒否であった場合、下位の設定もそれに従い拒否設定を行い、また、下位の設定が許可であるなら上位の設定も同様に許可となる。これは、情報を閲覧できるなら当然公開もされているし、更新が可能であるなら当然閲覧も可能だし、公開もされているはずであるからである。よってこの3設定は階層毎に矛盾がないような設定を行う方式となる。

【００３５】

なお、上記公開設定52、Read設定53、Write設定の他、パーミッションの設定種別は、図２の管理コンソールを介して、プレゼンスサーバのユーザが自由に設定することが可能である。例えば。公設定種別の数を増やせば、よりきめ細かな開示レベルを設定することが可能であるし、逆に隠蔽機能が不要な場合は、公開設定というパラメータを削除することもできる。いずれにせよ、本実施例では、オブジェクト情報を複数に分類し、かつ上下関係を与えて管理することで、オブジェクト情報の適切な管理を可能としている。

【００３６】

図６、図７、図８、は本願発明のプレゼンスサーバ1が実際に記憶するパーミッションを設定するためのエントリテーブルの例である。プレゼンスサーバ1は各ユーザが設定したパーミッション情報を図２の24に示す様なメモリ領域に記憶する場合、テーブル61、71、81の3つのテーブルで記憶を行う。以下では、プレゼンスサーバ1が各ユーザからパーミッション設定要求を受信し、その内容を記憶する時の動作を説明する。

【００３７】

まず図６の61に示すテーブル内部の公開ユーザ名フィールド62の中から情報を公開するユーザのユーザＩＤを検索し、それに対応したインデックス63を読み出す。ここで公開ユーザ62とはオブジェクト情報を公開するユーザのことを指す。

簡単には、オブジェクト情報に基づく何らかのサービスをサービス提供者から受けているユーザと考えてもよい。

【００３８】

図７はオブジェクト情報を開示する第三者と当該オブジェクト情報に対するパーミッションの設定値とが記録されたエントリテーブルである。図７のエントリテーブルは、図６に示されたインデックス毎に存在する。例えば、公開ユーザ名がUser Aのユーザは、インデックス1で識別されるパーミッション設定用のエントリテーブルを持っている。User Bはインデックス2のエントリテーブルを持っている。User C以下も同様である。

【００３９】

プレゼンスサーバ1は、71に示すインデックステーブルの内、読み出したインデックス番号に対応したテーブルから閲覧ユーザ名フィールドを検索し、それに対応したパーミッション設定内容73にパーミッション設定を書き込む。ここで閲覧ユーザ72とは公開ユーザが公開するオブジェクト情報を参照，もしくは公開ユーザの代理で更新するユーザ，またはアプリケーションサーバのことを指す。閲覧ユーザ名フィールドを検索した結果，閲覧ユーザ名を見つけることが出来なかった場合，新規のパーミッション設定とみなし，新たな閲覧ユーザ名とパーミッション設定内容をインデックステーブル７１の各フィールドに追加する。また，ユーザからの設定要求がパーミッションの削除であった場合，インデックステーブル７１から指定された閲覧ユーザ名を閲覧ユーザフィールド７２から削除，さにそれに対応したパーミッション設定内容フィールド７３も削除する。

【００４０】

また、プレゼンスサーバ1がユーザからパーミッション設定の取得要求を受信し、その内容を読み出す時も同様の動作を行い、パーミッション設定内容73からパーミッション設定を読み出す。また、インデックステーブル71は情報を公開するユーザ分用意する。つまり公開ユーザ毎にインデックステーブルを持つ形式となる。このテーブル71には閲覧ユーザ72とその閲覧ユーザに対するパーミッション設定内容73が記述されている。73のパーミッション設定は例えば64ビットの2進数の列で記述されている。この2進数の記述には先頭から2ビットずつ各情報に

対するパーミッションを設定する。

【００４１】

新たな公開ユーザを追加する場合，エントリテーブル61に公開ユーザ名を追加する。この時インデックスフィールド６３に記述するインデックス番号はサーバが空き番号を把握し，自動的に設定する。また，その時に新規追加した公開ユーザ用のインデックステーブル７１を用意する。逆に，現在登録されている公開ユーザを削除する場合はまず削除するユーザのインデックステーブル７１を消去し，その後，エントリテーブル６１の公開ユーザ名フィールド６２から削除するユーザ名を検索，その情報を削除する。

【００４２】

図８には、図７に示したパーミッションの設定内容をサーバが解釈する際の参照用テーブルを示す。図８の参照用テーブル81は、番号フィールド82と設定対象情報フィールド83で構成されている。番号フィールド82はパーミッション設定内容73の先頭から何番目の2ビットかを示す番号であり、設定対象情報フィールド83はその2ビットがどの情報に対するパーミッションかを記述している。テーブル81はこのようにパーミッション設定内容73とテーブル81を組み合わせてどの情報にどのようなパーミッションが設定されているかを読み出す、もしくは書き込むことが可能となっている。2ビットの2進数には、以下の4パターンのパーミッションを設定することが可能である。

１）公開設定52とRead設定53とWrite設定54すべてが拒否の設定、

２）公開設定52が許可でRead設定53とWrite設定54が拒否の設定、

３）公開設定52とRead設定53が許可でWrite設定54が拒否の設定、

４）すべてのパーミッションレベルが許可の設定、

例えば、上記１）の状態には設定値00を、上記２）には01を、上記３）には10を、上記４）には11を対応させることで、種々のパーミッションレベルの設定値を表現することが可能である。また、本実施例では、パーミッションレベルとして、公開設定可否、Read可否、Write可否の３つの状態を想定しているが、パーミッションレベルをより細分化し、設定レベルを４つ以上にする場合であっても、2進数のビットで各レベルの状態を表現することが可能である。例えば、3ビッ

トの2進数を用いれば、2^3=8種類のパーミッションレベルの設定を行なうことができる。

【００４３】

新たなオブジェクト情報を追加する場合，参照用テーブル８１に新しくエントリを追加する。エントリを追加することで今まで利用していなかったインデックステーブル７１のパーミッション設定内容フィールド７３に示すビット列にオブジェクト情報に対するパーミッション設定を割当てることが出来る。逆にオブジェクト情報を削除する場合は参照用テーブル８１からエントリを削除する。エントリが削除されたビット列はパーミッション設定，パーミッション取得時に参照されることが無くなり，未使用ビット列となる。

【００４４】

以上、本実施例では、パーミッションの設定値に対し、上下関係の表現が可能な数値コードを与えることにより、パーミッションレベルの上下関係を考慮した管理を可能としている。

【００４５】

パーミッション設定テーブルは、バックアップ等の目的で、外部のデータベース等に保存しておくことができる。図９には、外部記憶手段に格納するためのパーミッション設定テーブルの形式を示した。テーブル91は公開ユーザ名フィールド92、閲覧ユーザ名フィールド93、パーミッション設定内容フィールド94から構成されており、テーブル61、71と同様の内容を記述する。テーブル81の設定対象情報については、例えば、サーバの設定ファイルにバックアップ等のために保存しておく方法がある。

【００４６】

図１０はプレゼンスサーバ1がユーザからのパーミッション設定要求を受信した時、図１のパーミッション設定内容整合部9で行う処理の内容を示したフローチャート図である。パーミッション設定内容整合部9はユーザからのパーミッション設定要求の内容から図４、図５に示した上下関係に矛盾しないパーミッション設定内容を計算し、設定内容の整合を行う処理ブロックである。このブロックの動作について説明する。

【００４７】

パーミッション設定内容整合部9は、ステップ101でユーザのパーミッション設定要求を受信するとステップ102で処理を開始する。処理を開始するとまず、ステップ103でユーザからのパーミッション設定要求が図４、図５に示した上下関係と矛盾していないかをチェックする。もし矛盾を発見した場合、ステップ104でエラー出力を行い、ステップ119で処理を終了させ、ステップ120でユーザにパーミッション設定が失敗したことを示すメッセージを返信する。矛盾が無かった場合はステップ105でまずパーミッションを設定する。但し、一度に複数のオブジェクト情報に対するパーミッション設定要求があった場合、まずは一番始めに記述された設定について処理を行う。次にステップ106で設定要求に従い設定を行ったパーミッションについて図５に示した処理単位での上下関係の整合性を取るため、処理単位での上位パーミッションをチェックする。例えば設定要求がWrite設定に対するパーミッション設定であればRead設定についてチェックを行う。しかし、設定要求が最上位の公開設定である可能性もあるので、ステップ107で設定要求が処理単位の最上位であるかをチェックする。もし最上位であれば、ステップ111に進むが、最上位でなければステップ108に進み、チェック中処理単位と上位の処理単位の設定内容を比較する。ステップ108では、もし上位のパーミッション設定が拒否で、かつチェックしているパーミッション設定が許可であった場合、図５の上下関係に矛盾するので上位のパーミッションをステップ109で許可に設定する。矛盾が無ければこの処理は行わない。

【００４８】

次に、ステップ110でパーミッションのチェック対象を1階層上位に移動させる。例えば、現在Write設定をチェックしていたら、本ステップでチェック対象をRead設定に移動させる。その後はステップ106～をもう一度実行して、最上位の公開設定まで処理をループさせる。最上位までチェックを終えると、ステップ107にてループが終了してステップ111に処理が進む。ちなみにこのステップ106～ステップ110までの処理ループは図５に示す処理単位の上下関係を理解しながら行わなくてはならないが、上下関係についてはプレゼンスサーバ1のレジスタに予め設定されている。

【００４９】

ステップ111では今パーミッション設定をしているオブジェクト情報の設定内容とその上位のオブジェクト情報に現在設定されているパーミッションの内容との矛盾を整合する。現在パーミッション設定を行っているオブジェクト情報が図４に示す情報単位階層の最上位であるユーザＩＤである可能性があるので、まずステップ111で情報単位の最上位であるかをチェックする。もし現在設定しているオブジェクト情報が最上位であれば処理はステップ116に進む。もしそうでなければ、ステップ113で現在パーミッション情報を設定しているオブジェクト情報と図４で示された上下関係図での上位のオブジェクト情報に設定されているパーミッション設定のRead設定を比較する。もし上位オブジェクト情報のRead設定が拒否で今設定したオブジェクト情報のRead設定が許可であった場合、上位のオブジェクト情報は閲覧を拒否しているのに下位のオブジェクト情報の閲覧を許可しているという矛盾した状態になるので、ステップ114で上位のオブジェクト情報の公開設定、Read設定を許可にする。これで上下関係の矛盾を整合できる。もしステップ113で条件に当てはまらなかったらステップ114の処理は行われない。

【００５０】

この処理が終了するとステップ115でパーミッションチェック対象を現在のオブジェクト情報の1階層上位のオブジェクト情報に移動させ、ステップ111からの処理を再度行い、最上位であるユーザＩＤにパーミッションチェック対象が移動するまで処理をループさせる。最上位までパーミッションチェック対象が移動するとステップ112からステップ116に処理が進む。ちなみにこのステップ111～ステップ115までの処理ループは図４で示したオブジェクト情報単位の上下関係を理解しながら処理しなくてはならないが、その情報は図２のオブジェクト情報上下関係設定テーブル27に記憶されている。この設定はプレゼンスサーバ1の運用でユーザが関係を自由に設定することが可能である。

【００５１】

処理が進むとステップ116で全設定が終了したかをチェックする。ユーザからのパーミッション設定要求が複数のオブジェクト情報についてのみだった場合は、ステップ117に処理が進み、次に設定要求を読込み、その設定要求に対してス

テップ105からの処理を行う。すべての設定要求について処理を終えると、ステップ116からステップ118に処理が進み、整合したパーミッションの設定値をメモリに書き込む処理を行い、ステップ119で処理が終了する。その後、書き込み終了の通知を受信するとステップ120でユーザに対してパーミッション設定が成功したことを示すメッセージを返信する。

【００５２】

図１１はプレゼンスサーバ1がユーザからのパーミッション取得要求を受信した時、図１のパーミッション出力内容計算部10で行う処理の内容を示したフローチャート図である。パーミッション出力内容計算部10はユーザからのパーミッション取得要求を受けて、図２のパーミッション設定テーブル24からパーミッション設定を読み出した後、その設定が図４、図５に示した上下関係に矛盾しないかを確認して、もし矛盾があればパーミッション設定内容を計算し、計算後のパーミッション設定内容をユーザに返信する処理ブロックである。このブロックの処理方法について説明する。パーミッション出力内容計算部10はステップ131でユーザからパーミッション情報取得要求を受信すると、ステップ132で処理を開始する。処理を開始するとまず、ステップ133でパーミッション取得を要求してきたユーザが要求先のパーミッション設定を取得できるかをチェックする。もし取得権利がない場合、ステップ134に処理が進みエラー出力を行い、ステップ149で処理を終了し、ステップ150でパーミッション設定取得要求を送信したユーザに対して取得権利がないことを通知する。ステップ133で権利があった場合はステップ135に処理が進む。ステップ135ではパーミッション設定テーブル24からパーミッション設定を読み出す。次にステップ136に進み、各オブジェクト情報に対する処理単位でのパーミッション設定に図５で示した上下関係に矛盾がないかチェックを行う。この時、複数のオブジェクト情報に対するパーミッション設定についてチェックを行う必要があるが、チェックを行う順番は図８のテーブル81の番号82の順番、つまり、図７のパーミッション設定内容73の最初の2ビットからパーミッション設定を読み出す。処理単位パーミッションチェックではまずステップ136でチェックを行う処理設定を最上位、つまり公開設定に移動させる。次にステップ1001に進みチェック中の処理設定が最下位であるかどうかをチェック

するが、1度目のループは最上位の公開設定をチェックしているので最下位ではなく、そのままステップ137に処理を進め、公開設定が拒否であるかどうかをチェックする。もし拒否であった場合はそれより下位、つまりRead設定、Write設定も当然拒否であるのでそのように設定する。もし許可であった場合は、ステップ138に処理が進み、パーミッションチェック対象を1階層下位に移動させる。例えば、現在チェック中の処理設定が公開設定なら1階層下位のRead設定にパーミッションチェック対象を移動させる。

【００５３】

その後処理をステップ1001に進め再開し、最下位の処理設定に移るまで処理をループする。もし処理が最下位となったらステップ1001からステップ140に処理が進む。ステップ140では全てのオブジェクト情報についてチェックが終了したかを見て、もし終了していなければステップ141に処理を進め、次のオブジェクト情報についての設定を読込み、ステップ136からの処理を行う。終了している場合、次のステップ142に処理を進める。ステップ142ではオブジェクト情報単位で図４に示した上下関係に矛盾がないかチェックを行う。この処理ではまずステップ143でチェックを行うオブジェクト情報をユーザＩＤに移動させる。その後、ステップ1002でチェック中のオブジェクト情報が最下位であるかをチェックするが、現在のチェック中オブジェクト情報は最上位のユーザＩＤであるので、そのままステップ144に進み、チェック中のパーミッション設定のRead設定が拒否であるかどうかを見る。もし拒否であったら下位のオブジェクト情報についても見せる意思が無いと捕らえることが出来るので、ステップ146ですべての下位のオブジェクト情報に対して全処理設定の内容を拒否に設定する。もしステップ144でRead設定が許可であった場合、処理はステップ145に進む。ステップ145ではパーミッションチェック対象を処理単位で下位に移動させる。但し、ユーザＩＤの下位に位置するオブジェクト情報は複数存在することがある。その場合は下位のオブジェクト情報を任意に選びそのオブジェクト情報にパーミッションチェック対象を移す。この時チェックした下位のオブジェクト情報は記憶しておく。その後ステップ144を再開し、最下位のオブジェクト情報をチェックするまで処理をループさせる。

【００５４】

最下位のオブジェクト情報のチェックに移動したとき、ステップ1002からステップ147に処理が進む。ステップ147では記憶されたチェック済みの下位オブジェクト情報から、図４のツリー構造の全ての枝についてチェックを行ったかを調査し、もし全ての枝についてチェックを行っていなかった場合、ステップ148に処理を進める。ステップ148ではまだチェックを行っていない枝のオブジェクト情報にパーミッションチェック対象を移動させる。その後処理はステップ1002に進みすべての枝についてパーミッションチェックが終了するまで処理をループさせる。ステップ147で全ての枝についてのパーミッションチェックが終了していたら、処理はステップ149に進み終了する。その後、ステップ150でチェックを行ったパーミッション情報をユーザに返信する。なお、パーミッション出力内容計算部10が行う図１１の処理は必須の処理ではない。パーミッション設定内容整合部9の処理を信頼し、さらにその他のパスでパーミッション設定がパーミッション設定テーブル24に書き込まれない保障があるなら図１１で示した処理フローを実行せず、パーミッション設定テーブル24から取得してきたパーミッション設定をそのままユーザに送信しても良い。ただ、図１１に示す処理フローを実行することで情報公開ユーザが意図しなかった情報が流出してしまう可能性をより低くすることが出来る。

【００５５】

図１２は、本実施例のプレゼンスサーバを用いたサービスモデルの１例である。図１２において154で示すUser Aはプレゼンスサーバ1に情報を登録して、家族情報通知サーバ152からサービスを受けるユーザである。このサービスは家族情報通知サーバがUser Aとその家族の現在情報を把握し、例えばUser Aとその家族が持つ図１６の位置情報216がお互いに近くなったら家族情報通知サーバからアラームを通知するようなサービスである。本１２では、プレゼンスサーバは通信キャリアが所有しており、家族情報通知サーバ152および情報配信サーバ153はサービス提供業者が所有しているとの前提で記載されているが、通信キャリアが家族情報通知サーバ152および情報配信サーバ153を保有しており、事業として本サービスを行なう場合もあり得る。

【００５６】

サービスモデル全体の動作を説明すると、まず154で示すUser Aは自分の情報と自分の情報公開設定をプレゼンスサーバ1に登録し、家族情報通知サーバ152にサービス提供要求を行い、情報配信サーバ153を経由してサービスを受信する。本サービスモデルのその他の応用例としては、家族全員が今欲しい物を登録しておき、それを売っている店に近づいた他の家族にそれを通知する等の応用が可能である。

【００５７】

図１４には、その具体的な動作シーケンスを示す。以下では、その動作について説明する。154で示すUser Aはまず、ステップ171で家族情報通知サーバ152にサービス登録要求を送信する。すると、家族情報通知サーバ152はステップ172で4で示すUser Aに公開可能な情報について問い合わせを行う。4で示すUser Aはそれに対してステップ173において自分が公開できる情報を家族情報通知サーバ152に登録する。また、それと同時にステップ174においてプレゼンスサーバ1にもパーミッション設定を登録する。プレゼンスサーバ1は4で示すUser Aが登録してきた情報公開設定をステップ175でサーバ内部に保存する。また、家族情報通知サーバ152は4で示すUser Aの情報更新と更新された情報の内容について通知を受けるためにステップ176でUser Aの情報更新通知予約をプレゼンスサーバ1に対して行う。その後、4で示すUser Aは自分の情報の更新をステップ177でプレゼンスサーバ1に登録する。プレゼンスサーバ1は家族情報通知サーバ152からステップ176でUser Aの情報更新通知予約を受信してそれを享受しているので、家族情報通知サーバ152に対して更新通知を行おうとする。この時、プレゼンスサーバ1はまず、4で示すUser Aが家族情報通知サーバ152に対して設定しているパーミッション設定をステップ178で確認する。その後、パーミッション設定でRead設定が許可であることを確認した情報のみをステップ179で家族情報通知サーバ152に通知する。この際、通知方法には更新された情報についてのみを通知する方法と更新されていない情報を含め4で示すUser Aが持つ情報をすべて通知する方法の2通りが存在するがそれについてはどちらの方法を用いてもかまわない。

【００５８】

図１６に、4で示すUser Aが持つ情報と家族情報通知サーバ152に通知される情報についての一例を示す。図１６では4で示すUser Aはユーザ ＩＤ212、User Aが所持する端末1のＩＤ213、User Aが所持する2台目の端末2のＩＤ214、また端末2に付随する情報であるＯｎ／Ｏｆｆ215、位置216を保有しているとする。しかし家族情報通知サーバ152に対しては4で示すUser Aのユーザ情報212、214、215、216しか見えていない。User Aはパーミッション設定テーブル22に家族情報通知サーバ152に対して端末1のＩＤ213の公開設定を拒否と登録しており、プレゼンスサーバ1のパーミッション管理部3が端末1のＩＤ213を通知しなかったためである。また、情報更新通知の方法が更新された情報のみを通知する方法の場合、その更新された情報が4で示すUser Aの家族情報通知サーバ152に対するパーミッション設定の公開設定、もしくはRead設定を拒否としていた場合にはステップ179の情報更新通知は行わない。家族情報通知サーバ152はステップ179で4に示すUser Aの更新された情報を入手してステップ180でその更新された情報、また、他の更新されてない情報を含めて確認してサービス提供判断、その内容の判断を行う。その後、家族情報通知サーバ152はサービス配信を決定するとステップ181で情報配信サーバ153にサービスの配信要求を送信する。その後は情報配信サーバ153がステップ182において相手端末に合わせて動画や静止画、文字などの配信メディア、User Aの通信帯域に合わせたビットレート設定等を行い、ステップ183でUser Aに対してサービスを配信する。しかし、家族情報通知サーバ152はステップ180で更新取得したUser Aの情報を確認してサービス配信をしないことを決定するとステップ181～183までの処理は行なわず、次のUser Aの情報更新が通知されるまで待つ。また、このシーケンスにおいて家族情報通知サーバ152が配信サーバ153の機能を有することもある。この場合、ステップ181の処理は行われず、ステップ182、183の処理を家族情報通知サーバ152が行うこともある。

【００５９】

図１４は図１２の実施例をＳＩＰ（Session Initiation Protocol）／ＳＩＭＰＬＥ（SIP for Instant Messaging and Presence Leveraging Extensions）を用いて実現した例である。ＳＩＰ／ＳＩＭＰＬＥとはリアルタイム通信のセッション確立とプレゼンス情報の更新通知予約やそれに対する更新通知、ＩＭ等、マ

ルチメディアコミュニケーションを行うために必要な機能を提供するプロトコルである。図１４のＳＩＰサーバ161はこのＳＩＰ／ＳＩＭＰＬＥに準拠したメッセージをルーティングし、目的の相手まで転送する機能を持つ。

【００６０】

図１５は図14のシーケンスをＳＩＰ／ＳＩＭＰＬＥを用いて実現した適用例である。図１５ではＳＩＰ／ＳＩＭＰＬＥに加えてＨＴＴＰ（Hyper Text Transport Protocol）も用いてサービスを実現している。本シーケンスではサービス登録要求171、公開情報問い合わせ172、広報公開設定登録173をＨＴＴＰを用いた191、192、193で実現する。またパーミッション設定174はＳＩＭＰＬＥを適用してＭＥＳＳＡＧＥメソッド送信194でＳＩＰサーバ161を中継して実現している。メソッドとはＳＩＰ／ＳＩＭＰＬＥメッセージの一番始めの部分に記述する文字列であり、その文字列の確認によりそのＳＩＰ／ＳＩＭＰＬＥメッセージがどのような目的で送信されているかを判断することが可能となる。ちなみにＭＥＳＳＡＧＥメソッドは本来テキストベースＩＭの発言内容を送信するメソッドであるが、本願発明の装置ではパーミッション設定要求、取得要求ができるように拡張を行っている。また、User Aの情報更新通知予約176はＳＩＭＰＬＥのＳＵＢＳＣＲＩＢＥメッセージ送信196でＳＩＰサーバ161を中継して実現している。次の情報更新177はＲＥＧＩＳＴＥＲメッセージ送信197でＳＩＰサーバ161を中継して実現している。ＲＥＧＩＳＴＥＲメソッドは本来ユーザのオンライン登録を行うメソッドであるが、これについても本願発明の装置ではこのメソッドを利用してユーザ情報の登録が出来るように拡張している。

【００６１】

その後のUser Aの情報更新通知179はＮＯＴＩＦＹメッセージ送信199でＳＩＰサーバ161を中継して実現する。ＮＯＴＩＦＹメソッドはこのようにＳＵＢＳＣＲＩＢＥで享受したユーザ情報更新通知予約に対して情報更新を通知するためのメソッドである。その後のサービス送信183についてはリアルタイム性の高い動画や音声での配信の場合はＳＩＰを利用してＩＮＶＩＴＥメッセージ送信後、User A154と情報配信サーバ153の間にセッションを張った後にＲＴＰプロトコルを利用してサービスを転送する。静止画やテキストベースの様にリアルタイム性が

低い配信の場合はＳＩＭＰＬＥのＭＥＳＳＡＧＥメソッドを用いて文字情報を直接送信する方法で実現する。どちらの方法を取るにせよ、ＳＩＰサーバ161が中継してＳＩＰメッセージを転送する。

（実施例２）

図１７に、プレゼンスサーバを用いたビジネスモデルの第2の実施例を示す。図１７に224で示されるUser Aは、普段の買い物で○×デパートを利用することが多く、○×デパート購入履歴蓄積サーバ221にはUser Aの商品購入履歴が蓄積されている。また、User Aは図２１に示すユーザＩＤ272、ユーザに付随する情報として趣味273、年収274、端末のＩＤ276、端末に付随する情報としてＯｎ／Ｏｆｆ277、位置278をプレゼンスサーバ1に登録しており、店舗情報配信サーバ222からサービスを受けるユーザである。全体の動作を説明するとまずUser A224は自分のユーザ情報と店舗情報配信サーバ222に対するパーミッション設定をプレゼンスサーバ1に登録している。また、店舗情報配信サーバ222にサービス提供要求を行い、情報配信サーバ223を経由してサービスを受信する。

【００６２】

図１０はその動作シーケンスである。このシーケンスを用いて具体的な動作について説明する。224で示すUser Aはまず、ステップ231で○×デパート購入履歴蓄積サーバ221に自分の情報を登録する。具体的にはUser Aが○×デパートで買い物をする度に○×デパート購入履歴蓄積サーバ221にその履歴が蓄積されていく。○×デパート購入履歴蓄積サーバ221はその履歴をステップ232でプレゼンスサーバに登録する。User Aはステップ233により店舗情報配信サーバ222にサービス登録要求を送信する。すると、店舗情報配信サーバ222はステップ234によりUser Aに公開可能な情報について問い合わせを行う。User Aはそれに対してステップ235において自分が公開できる情報を店舗情報配信サーバ222に登録する。また、それと同時にステップ236においてプレゼンスサーバ1にも店舗情報配信サーバ222に対するパーミッション設定を登録する。

【００６３】

プレゼンスサーバ1はUser Aが登録してきたパーミッション設定をステップ237でサーバ内部に保存する。また、店舗情報配信サーバ222はUser Aの情報更新の

内容について通知を受けるためにステップ238でUser Aの情報更新通知予約をプレゼンスサーバ1に対して行う。その後、User Aは自分の情報の更新をステップ239によりアプリケーションサーバ1に登録する。プレゼンスサーバ1は店舗情報配信サーバ222からステップ238でUser Aの情報更新通知予約を受信してそれを享受しているので、ステップ240でUser Aが店舗情報配信サーバ222に対して設定したパーミッションを確認後、Read設定が許可であるユーザ情報についてのみステップ241で店舗情報配信サーバ222にUser Aの情報更新を通知する。この際、通知方法には更新された情報についてのみを通知する方法と更新されていない情報を含めUser Aが持つ情報をすべて通知する方法の2通りが存在するがそれについてはどちらの方法を用いてもかまわない。

【００６４】

図２１に、User Aがプレゼンスサーバ1、および○×デパート購入履歴蓄積サーバ221に登録、更新する情報と店舗情報通知サーバ222が受信するUser Aについての情報の一例を示す。図２１ではUser AはユーザＩＤ272、ユーザに付随する情報として趣味273、年収274、○×デパートの購入履歴274、User Aが所持する端末1のＩＤ276、端末1に付随する情報としてＯｎ／Ｏｆｆ277、位置278を保有している。しかし、店舗情報配信サーバ222はUser Aの年収情報に関して公開拒否281を受信している。これは、User Aが店舗情報配信サーバ222に対して年収のRead設定を拒否にしたパーミッション情報をプレゼンスサーバ1に登録していたからである。また、情報更新通知の方法が更新された情報のみを通知する方法の場合、その更新された情報の店舗情報配信サーバ222に対するパーミッションが公開設定、もしくはRead設定拒否であった場合、ステップ241の情報更新通知は行われない。

【００６５】

店舗情報配信サーバ222はステップ241でUser Aの更新された情報を入手してステップ242でその更新された情報、また、他の更新されてない情報を含めて確認してサービス提供判断、その内容の判断を行う。その後、店舗情報配信サーバはサービス配信を決定するとステップ243で情報配信サーバ223にサービスの配信要求を送信する。その後は情報配信サーバ223がステップ244において相手端末に合

わせて動画や静止画、文字などの配信メディア、User Aの通信帯域に合わせたビットレート設定等を行い、ステップ245でUser Aに対して例えばUser Aの現在位置のすぐ近くにある店舗情報やその店舗のサービスクーポンなどのサービスを配信する。この時、店舗情報配信サーバ222はステップ241で更新取得したUser Aの情報を確認してサービス配信をしないことを決定するとステップ243～245までの処理は行なわず、次のUser Aの情報更新が通知されるまで待つ。また、このシーケンスにおいて店舗情報配信サーバ222が配信サーバ223の機能を有することもある。この場合、ステップ243の処理は行われず、ステップ244、245の処理を店舗情報配信サーバ222が行うこともある。

【００６６】

図１８は、図１７の実施例をＳＩＰ（Session Initiation Protocol）／ＳＩＭＰＬＥ（SIP for Instant Messaging and Presence Leveraging Extensions）を用いて実現した例である。また、図２０は図１９のシーケンスをＳＩＰ／ＳＩＭＰＬＥとＨＴＴＰを用いて実現した例である。図２０を用いて図１８の具体的な動作について説明する。図１９ではUser Aの購入履歴登録232をＳＩＰのＲＥＧＩＳＴＥＲメッセージ送信252を用いてＳＩＰサーバ161を中継して実現している。次に、サービス登録要求233、公開情報問い合わせ234、公開情報登録235については253、254、255のステップでＨＴＴＰを利用して実現している。また、パーミッション設定登録236はＭＥＳＳＡＧＥメッセージ送信256でＳＩＰサーバ161を中継して実現する。次のUser Aの情報変更通知予約238はＳＵＢＳＣＲＩＢＥメッセージ送信258でＳＩＰサーバを中継して実現する。ユーザ情報更新239は232と同様ＲＥＧＩＳＴＥＲメッセージ送信259を利用してＳＩＰサーバ中継により実現する。情報更新通知241についてはＮＯＴＩＦＹメッセージ送信261でＳＩＰサーバを中継して実現する。また最後のステップであるサービス配信245はステップ265で動画などのリアルタイム性の高いメディア配信の場合はＩＮＶＩＴＥメッセージ送信後、セッションが張れた後にＲＴＰでサービス送信する。静止画、テキスト等リアルタイム性の低い配信の場合はＭＥＳＳＡＧＥメソッド送信により実現する。どちらの方法を取ってもＳＩＰメッセージはＳＩＰサーバ161を中継して転送される。

（実施例3）

図２２は、プレゼンスサーバを用いたビジネスモデルの第3の実施例を示す。User A301はプレゼンスサーバ1に図２５のユーザＩＤ312、ユーザに付随する情報として趣味313、年収314、User Aが所有する端末1のＩＤ315、端末1に付随する情報としてＯｎ／Ｏｆｆ316、位置317を登録している。また、User B302はUser Aの情報更新通知の予約を行い、User Aの現在状態を把握しているユーザである。図２４この実施例の動作シーケンス図である。この実施例の具体的な動作を図２４で説明する。まず、User Aはステップ321で趣味313をプレゼンスサーバ1に登録する。プレゼンスサーバ1は趣味313をデータベースサーバＡ303－1に保存する設定としているので、ステップ322でこれをデータベースサーバＡ303－1に登録する。

【００６７】

次にUser Aはステップ323で端末1に付随する位置316をプレゼンスサーバ1に登録する。プレゼンスサーバ1は位置316をデータベースサーバＢ303－2に保存する設定としているので、ステップ324でUser Aの位置316をデータベースサーバＢ303－2に登録する。その後User Aはステップ325でUser Bに対するパーミッション設定をプレゼンスサーバ1に登録する。するとプレゼンスサーバ1はステップ326でUser AのUser Bに対するパーミッション設定を記憶する。その後、User BがUser Aの情報更新を知るためにプレゼンスサーバ1に対してステップ327でUser Aの情報更新通知予約を送信する。そこでプレゼンスサーバ1はステップ328でUser AがUser Bに対して設定したパーミッションをまず確認してRead設定が許可のユーザ情報についてのみUser Bに通知を行う。そのためにプレゼンスサーバ1はReadが許可された情報のみをステップ329と330でデータベースサーバＡ303－1とデータベースサーバＢ303－2からUser Aのユーザ情報を読み出し、ステップ331でUser Bに通知を行う。この時、もしユーザＩＤの公開設定、もしくはRead設定が拒否である場合は通知できるユーザ情報が無いのでステップ331では権利が無いことを返信してこの動作シーケンスは終了する。その後、User Aがステップ332で例えば位置情報と趣味を更新するとプレゼンスサーバ1はステップ333、334でそれぞれのユーザ情報を保存しているデータベースサーバＡ303－1、データベース

サーバＢ303－2に保存、また、ステップ335でUser AがUser Bに対して設定しているパーミッション情報を確認してRead設定が許可のユーザ情報をステップ336でUser Bに通知する。

【００６８】

図２５の302を見るとUser Bに通知されるUser Aの情報の内ユーザに付随する年収351、端末1に付随する位置352は公開拒否となっている。これはUser AがUser Bに対して年収と位置のRead設定が拒否のパーミッション設定をパーミッション設定テーブル24に登録しており、プレゼンスサーバ1のパーミッション制御部3が公開拒否通知を判断したためである。

【００６９】

また、図２３は図２２の実施例をＳＩＰ／ＳＩＭＰＬＥで実現した例である。2つの図面ではプレゼンスサーバ1からデータベースサーバＡ303－1、データベースサーバＢ303－2の間のインターフェースは同様であるが、図２３ではUser A301からプレゼンスサーバ1、User B302からプレゼンスサーバ1へのインターフェースがＳＩＰ／ＳＩＭＰＬＥのＲＥＧＩＳＴＥＲ、ＳＵＢＳＣＲＩＢＥ、ＮＯＴＩＦＹ、ＭＥＳＳＡＧＥメソッドを利用したメッセージをＳＩＰサーバ161が中継する形となっている。

（実施例４）

実施例４では、プレゼンスサーバの別な構成例について説明する。図２６は、図２とは別構造のプレゼンスサーバを示した模式図である。本実施例のプレゼンスサーバは、公開ユーザ名と閲覧ユーザ名とパーミッションの設定値とをひとつにまとめたエントリテーブルを使用している。つまり、図９に示したエントリテーブルと同じエントリテーブルを使用している。本方式のエントリテーブルは、公開ユーザ名フィールド、閲覧ユーザ名フィールドおよびパーミッションの設定値フィールドとが一つのエントリテーブルにまとめられているため、図６，７のようにエントリテーブルを分けた場合に比べ、パーミッションの設定内容からユーザ名を検索する逆引きがやりやすいという利点を持つ。

【００７０】

但し、エントリテーブルのデータサイズが大きくなるため、図２に示した実施

例のようにメモリに全データを格納するのは不可能で、通常は外部記憶装置2002に格納しておき、必要な部分のみをメモリ空間上に展開して、パーミッションの設定処理を行っている。2001はディスクインタフェースであり、外部記憶装置2002とプレゼンスサーバ本体とを接続する。また、パーミッション設定内容を解釈するための参照用テーブル（図８と同じテーブル）は、本実施例においても必要であり、このため、本実施例のプレゼンスサーバは、参照用メモリを格納するためのキャッシュメモリ2003を備えている。

【００７１】

【発明の効果】

パーミッションのみを独立に管理するため、従来、新たなサービスに加入するたびに行っていたパーミッションの設定を簡略化でき、ユーザビリティが向上する。

【図面の簡単な説明】

【図１】

本願発明におけるパーミッション設定方式を適用した装置の機能ブロック図である。

【図２】

本願発明におけるパーミッション設定方式を適用した装置図である。

【図３】

本願発明装置で取り扱うユーザ情報の階層構造を示した図である。

【図４】

本願発明装置で行うパーミッション設定のユーザ情報単位での階層構造を示した図である。

【図５】

本願発明装置で行うパーミッション設定の処理単位での階層構造を示した図である。

【図６】

本願発明装置が記憶するパーミッション設定のテーブル図である。

【図７】

本願発明装置が記憶するパーミッション設定のテーブル図である。

【図８】

本願発明装置が記憶するパーミッション設定のテーブル図である。

【図９】

本願発明装置が外部に記録するパーミッション設定のテーブル図である。

【図１０】

本願発明装置がパーミッションを設定するときの処理フローチャート図である。

【図１１】

本願発明装置がパーミッションを読出しするときの処理フローチャート図である。

【図１２】

本願発明装置を用いたサービスのネットワーク図である。

【図１３】

本願発明装置を用いたサービスのＳＩＰサーバを用いた時のネットワーク図である

【図１４】

本願発明装置を用いたサービスの動作シーケンス図である。

【図１５】

本願発明装置を用いたサービスのＳＩＰサーバを用いた時の動作シーケンス図である。

【図１６】

本願発明装置を用いたサービスで伝達されるユーザ情報を示した図である。

【図１７】

本願発明装置を用いたサービスのネットワーク図である。

【図１８】

本願発明装置を用いたサービスのＳＩＰサーバを用いた時のネットワーク図である。

【図１９】

本願発明装置を用いたサービスの動作シーケンス図である。

【図２０】

本願発明装置を用いたサービスのＳＩＰサーバを用いた時の動作シーケンス図である。

【図２１】

本願発明装置を用いたサービスで伝達されるユーザ情報を示した図である。

【図２２】

本願発明装置を用いて複数のデータベースサーバを取り扱った場合のネットワーク図である。

【図２３】

本願発明装置を用いて複数のデータベースサーバを取り扱いＳＩＰサーバを利用した場合のネトワーク図である。

【図２４】

本願発明装置を用いて複数のデータベースサーバを取り扱った場合の動作シーケンス図である。

【図２５】

本願発明装置を用いて複数のデータベースサーバを取り扱った場合の伝達される情報を示した図である。

【図２６】

本願発明の情報管理装置の第２の実施形態である。

【図２７】

Ｕｎｉｘファイルシステムにおけるパーミッションの管理方式を説明する図である。

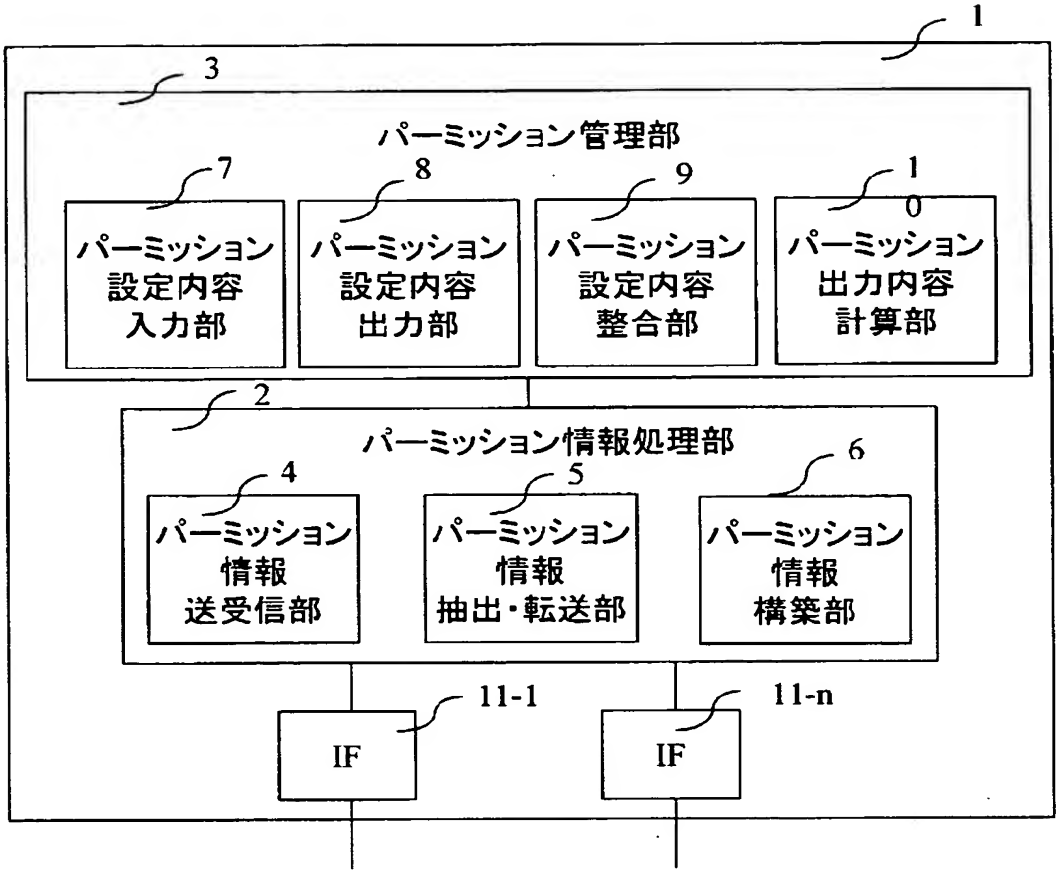
【符号の説明】

１・・・プレゼンスサーバ、２・・・パーミッション情報制御部、３・・・パーミッション管理部、

【書類名】　図面

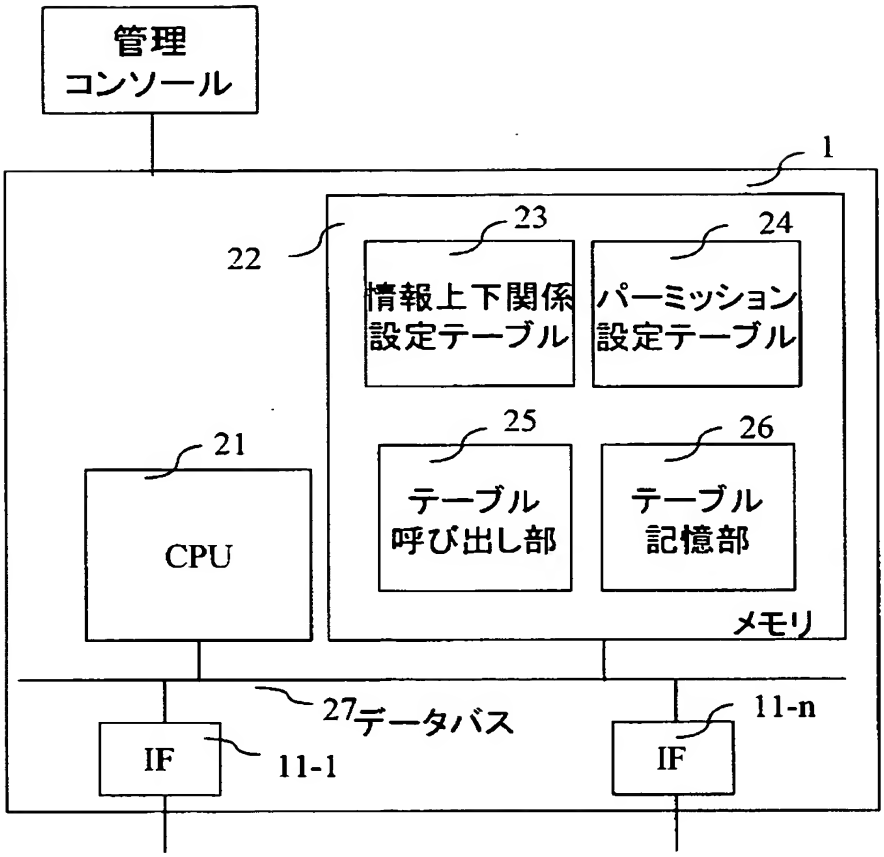
【図１】

図1


1
3
パーミッション管理部
7
パーミッション
設定内容
入力部
8
パーミッション
設定内容
出力部
9
パーミッション
設定内容
整合部
10
パーミッション
出力内容
計算部
2
パーミッション情報処理部
4
パーミッション
情報
送受信部
5
パーミッション
情報
抽出・転送部
6
パーミッション
情報
構築部
11-1
IF
11-n
IF

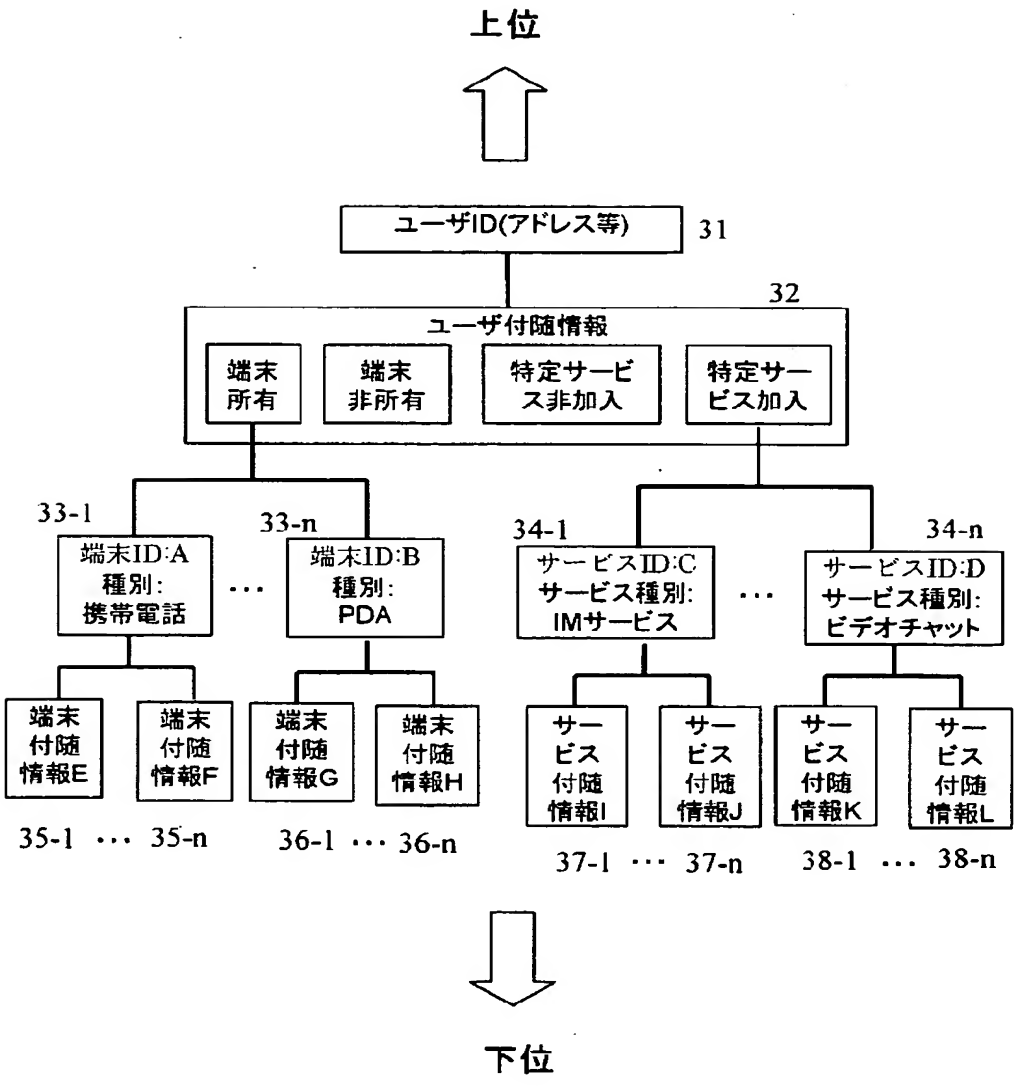
【図２】

図２


管理
コンソール
1
22
23
情報上下関係
設定テーブル
24
パーミッション
設定テーブル
25
テーブル
呼び出し部
26
テーブル
記憶部
21
CPU
メモリ
27データバス
IF
11-1
IF
11-n

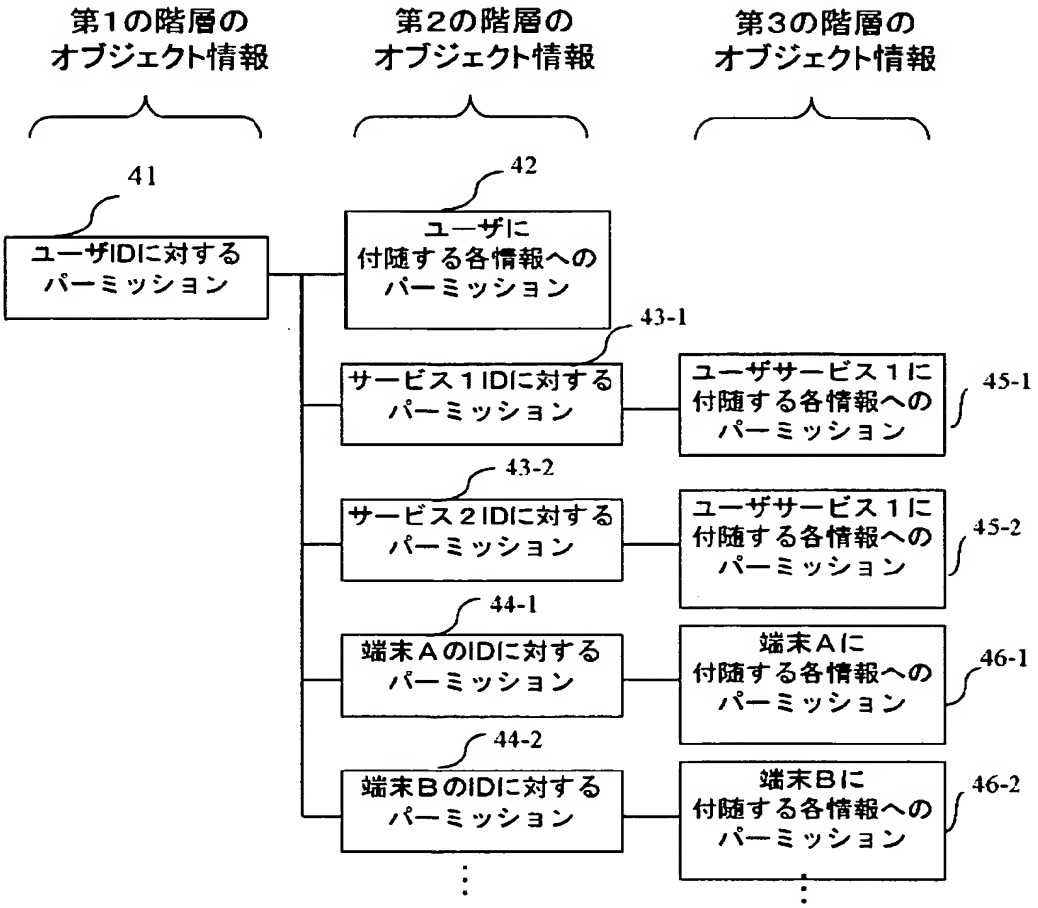
【図３】

図3


上位
ユーザID(アドレス等)
31
32
ユーザ付随情報
端末所有
端末非所有
特定サービス非加入
特定サービス加入
33-1
端末ID:A
種別:
携帯電話
33-n
端末ID:B
種別:
PDA
34-1
サービスID:C
サービス種別:
IMサービス
34-n
サービスID:D
サービス種別:
ビデオチャット
端末付随情報E
端末付随情報F
端末付随情報G
端末付随情報H
サービス付随情報I
サービス付随情報J
サービス付随情報K
サービス付随情報L
35-1 … 35-n
36-1 … 36-n
37-1 … 37-n
38-1 … 38-n
下位

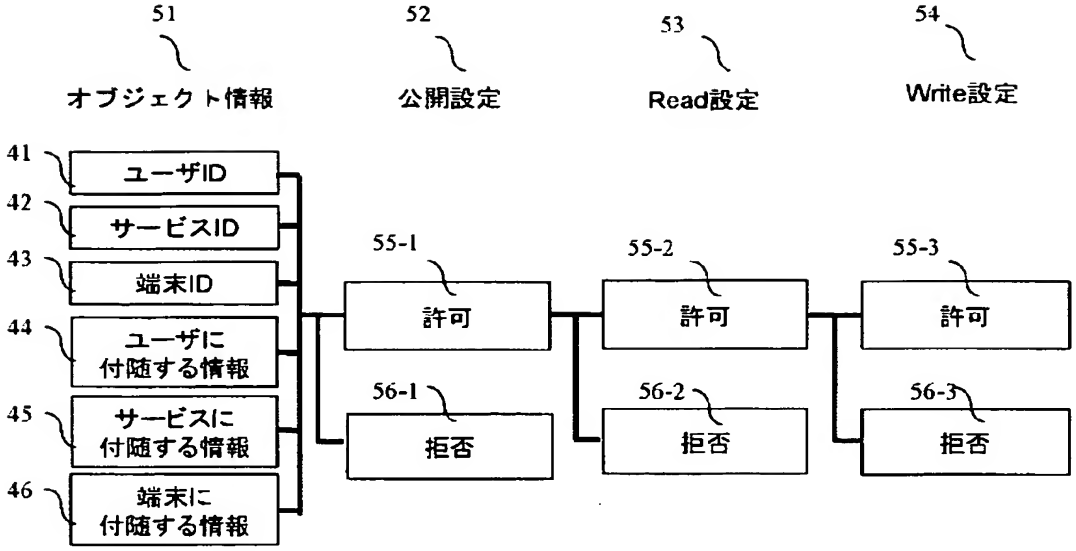
【図４】

図4


第1の階層の
オブジェクト情報
第2の階層の
オブジェクト情報
第3の階層の
オブジェクト情報
41
ユーザIDに対する
パーミッション
42
ユーザに
付随する各情報への
パーミッション
43-1
サービス１IDに対する
パーミッション
ユーザサービス１に
付随する各情報への
パーミッション
45-1
43-2
サービス２IDに対する
パーミッション
ユーザサービス１に
付随する各情報への
パーミッション
45-2
44-1
端末ＡのIDに対する
パーミッション
端末Ａに
付随する各情報への
パーミッション
46-1
44-2
端末ＢのIDに対する
パーミッション
端末Ｂに
付随する各情報への
パーミッション
46-2

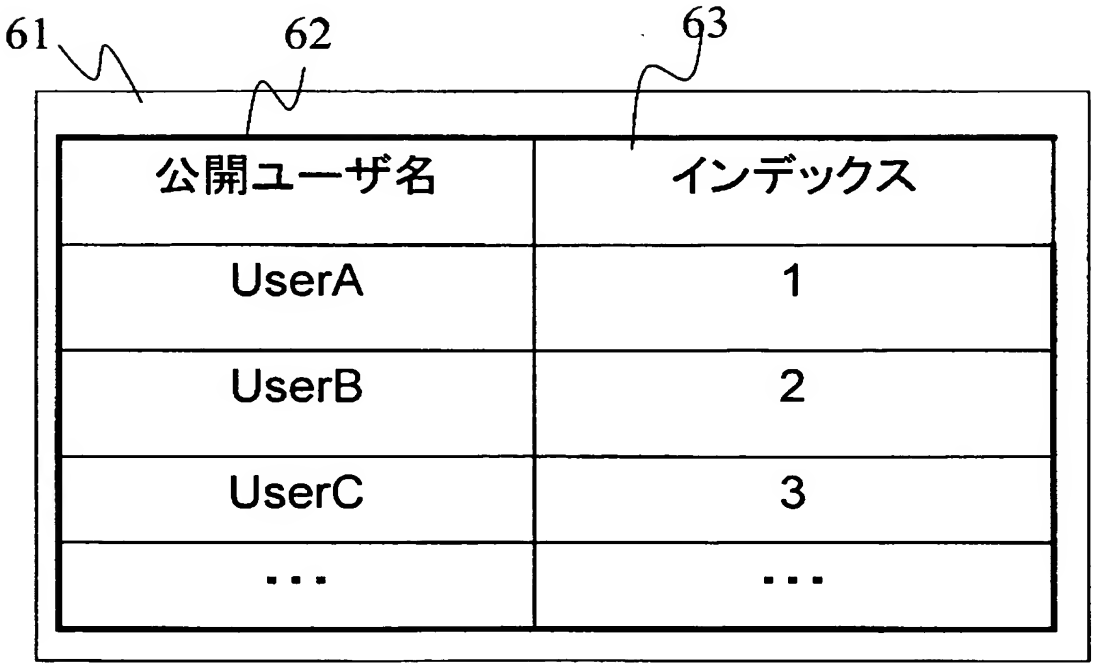
【図５】

図5


51
52
53
54
オブジェクト情報
公開設定
Read設定
Write設定
41
ユーザID
42
サービスID
43
端末ID
44
ユーザに
付随する情報
45
サービスに
付随する情報
46
端末に
付随する情報
55-1
許可
55-2
許可
55-3
許可
56-1
拒否
56-2
拒否
56-3
拒否

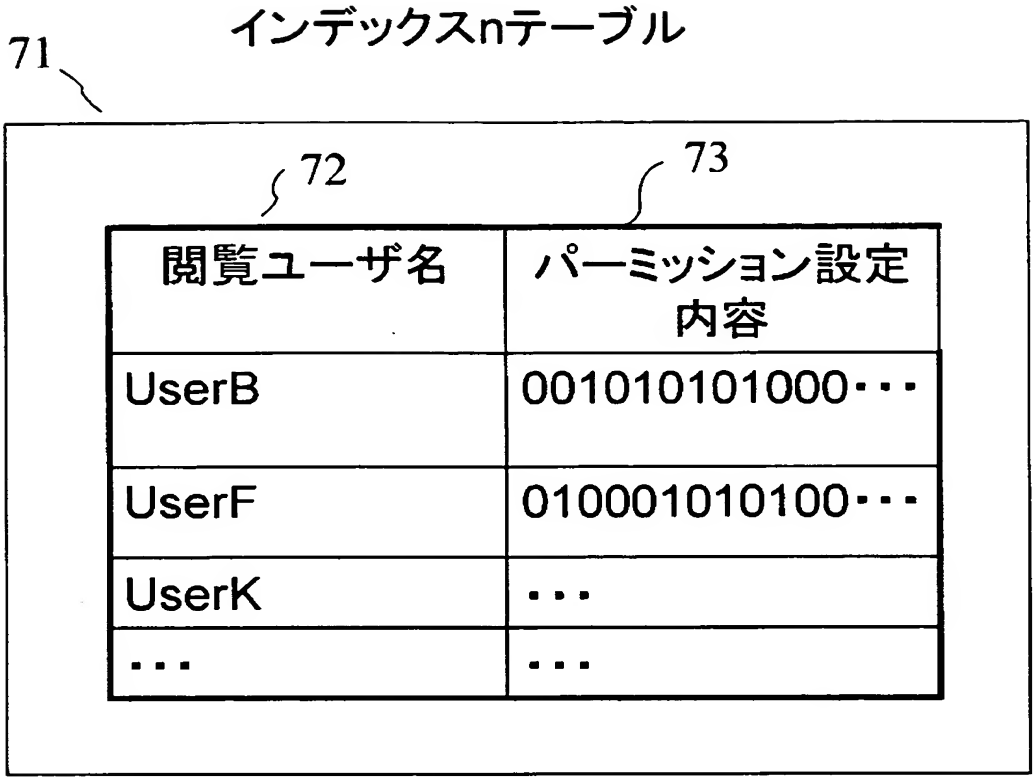
【図６】

図6


61
62
63
公開ユーザ名
インデックス
UserA
1
UserB
2
UserC
3
・・・
・・・

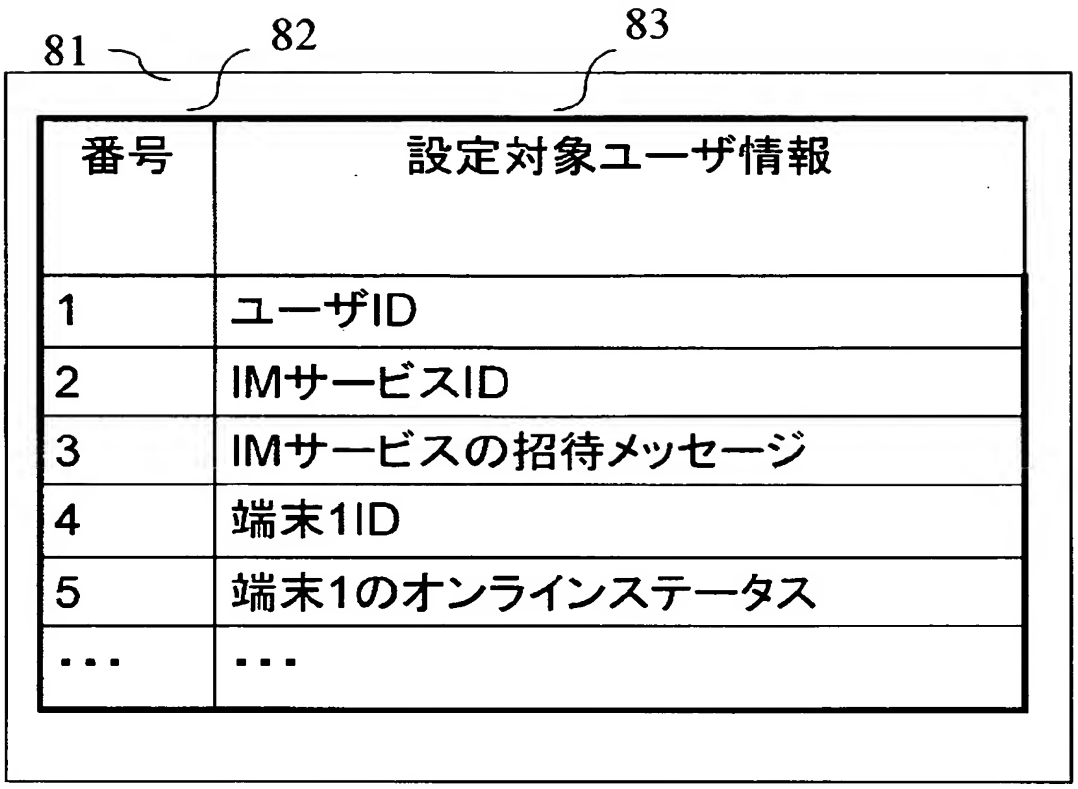
【図７】

図7


インデックスnテーブル
71
72
73
閲覧ユーザ名
パーミッション設定内容
UserB
001010101000・・・
UserF
010001010100・・・
UserK
・・・
・・・
・・・

【図８】

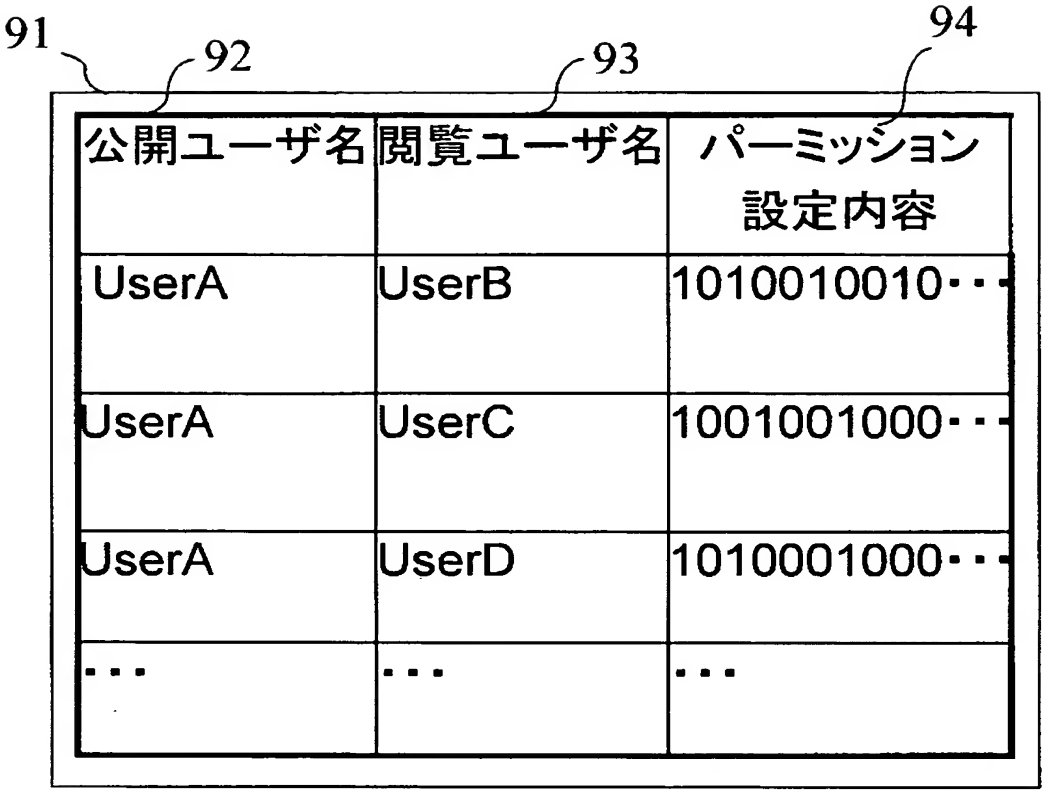
図8



番号	設定対象ユーザ情報
1	ユーザID
2	IMサービスID
3	IMサービスの招待メッセージ
4	端末1ID
5	端末1のオンラインステータス
・・・	・・・

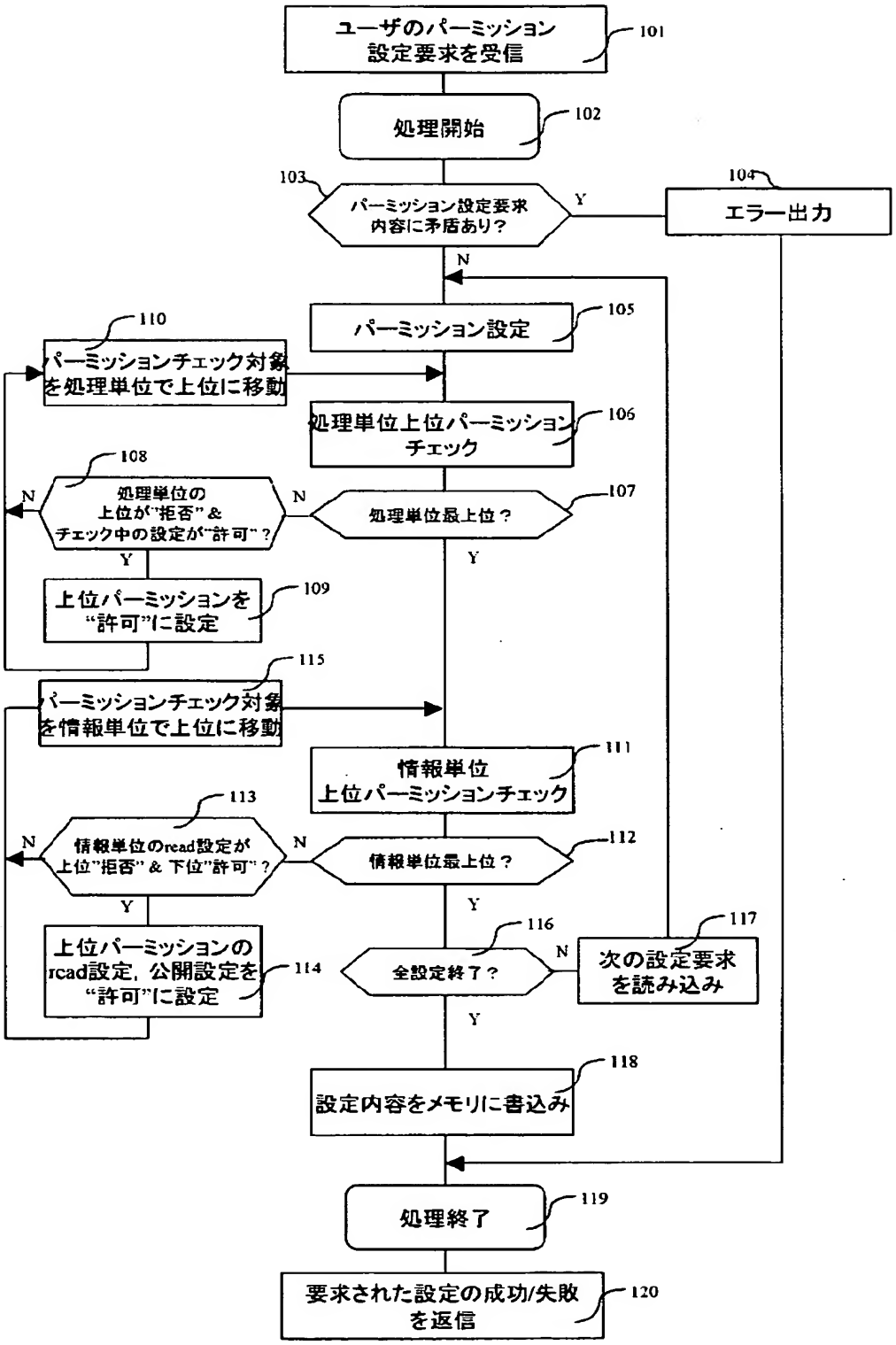
【図９】

図９


91
92
93
94
公開ユーザ名
閲覧ユーザ名
パーミッション設定内容
UserA
UserB
1010010010・・・
UserA
UserC
1001001000・・・
UserA
UserD
1010001000・・・
・・・
・・・
・・・

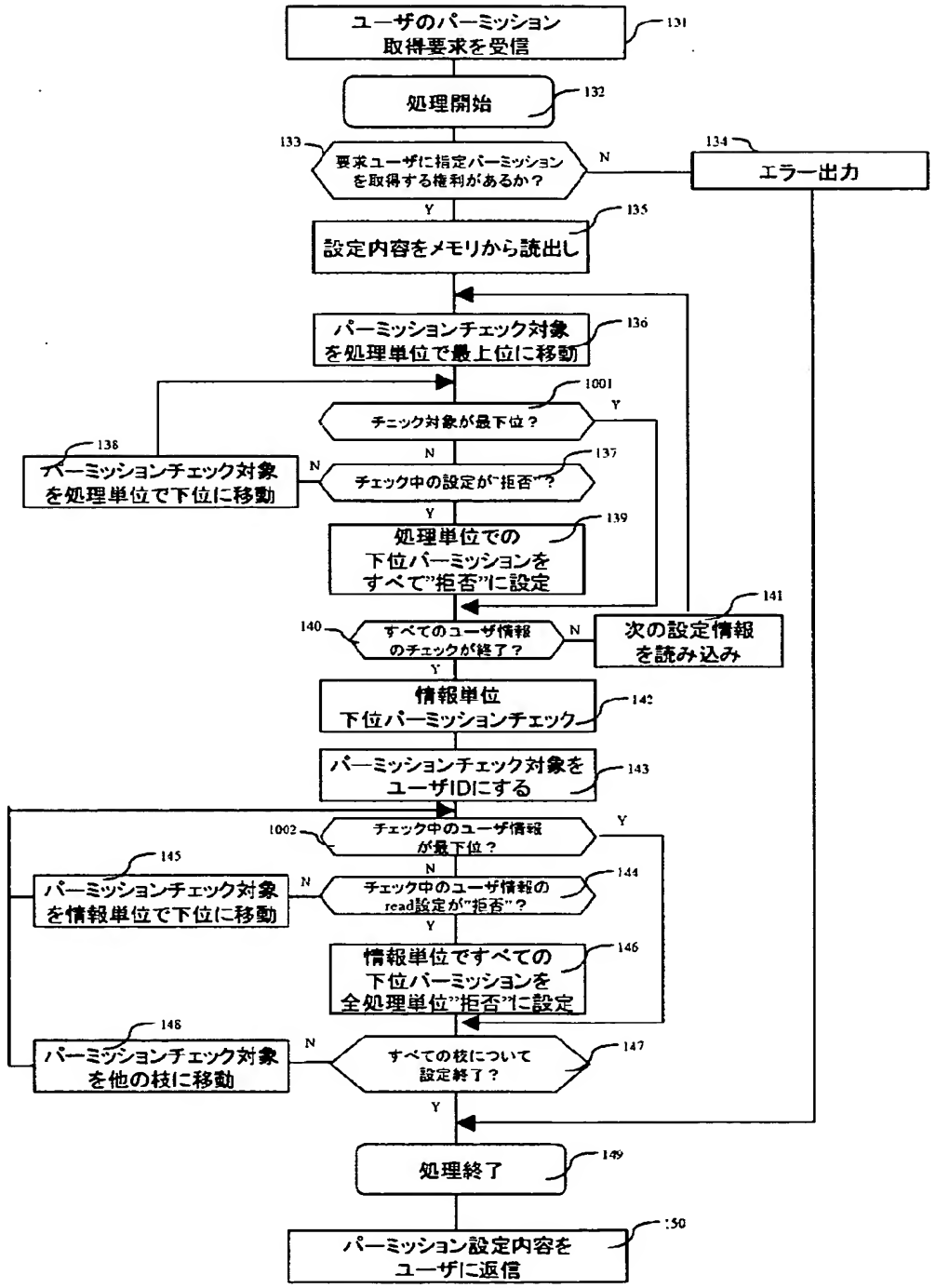
【図１０】

図10


ユーザのパーミッション設定要求を受信
101
処理開始
102
103
パーミッション設定要求内容に矛盾あり？
Y
104
エラー出力
N
パーミッション設定
105
110
パーミッションチェック対象を処理単位で上位に移動
処理単位上位パーミッションチェック
106
108
N
処理単位の上位が"拒否"＆チェック中の設定が"許可"？
N
処理単位最上位？
107
Y
Y
上位パーミッションを"許可"に設定
109
115
パーミッションチェック対象を情報単位で上位に移動
情報単位上位パーミッションチェック
111
113
N
情報単位のread設定が上位"拒否"＆下位"許可"？
N
情報単位最上位？
112
Y
Y
116
117
上位パーミッションのread設定，公開設定を"許可"に設定
114
全設定終了？
N
次の設定要求を読み込み
Y
118
設定内容をメモリに書込み
処理終了
119
要求された設定の成功/失敗を返信
120

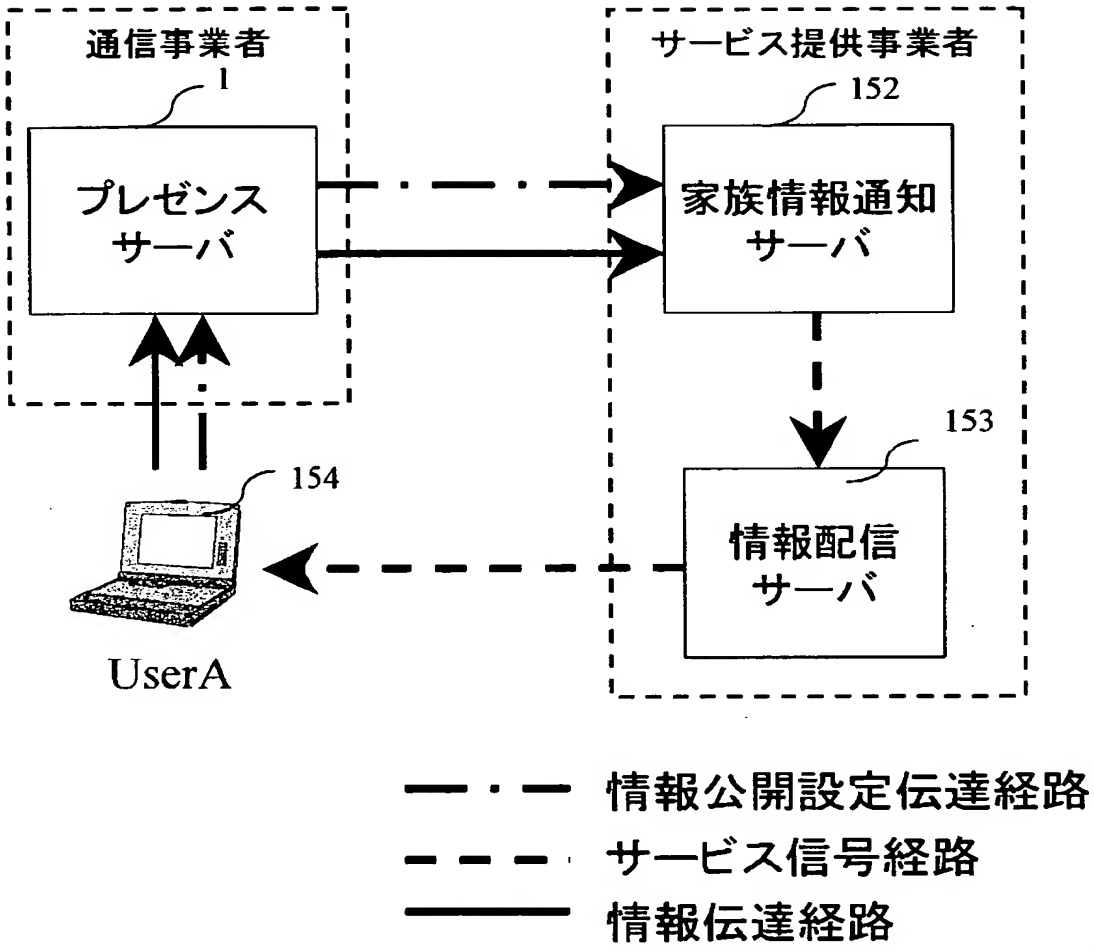
【図１１】

図11


ユーザのパーミッション取得要求を受信
131
処理開始
132
133
要求ユーザに指定パーミッションを取得する権利があるか？
N
134
エラー出力
Y
135
設定内容をメモリから読出し
パーミッションチェック対象を処理単位で最上位に移動
136
1001
チェック対象が最下位？
Y
N
138
パーミッションチェック対象を処理単位で下位に移動
N
137
チェック中の設定が"拒否"？
Y
139
処理単位での下位パーミッションをすべて"拒否"に設定
141
140
すべてのユーザ情報のチェックが終了？
N
次の設定情報を読み込み
Y
情報単位下位パーミッションチェック
142
パーミッションチェック対象をユーザIDにする
143
1002
チェック中のユーザ情報が最下位？
Y
N
145
パーミッションチェック対象を情報単位で下位に移動
N
144
チェック中のユーザ情報のread設定が"拒否"？
Y
146
情報単位ですべての下位パーミッションを全処理単位"拒否"に設定
148
パーミッションチェック対象を他の枝に移動
N
147
すべての枝について設定終了？
Y
処理終了
149
150
パーミッション設定内容をユーザに返信

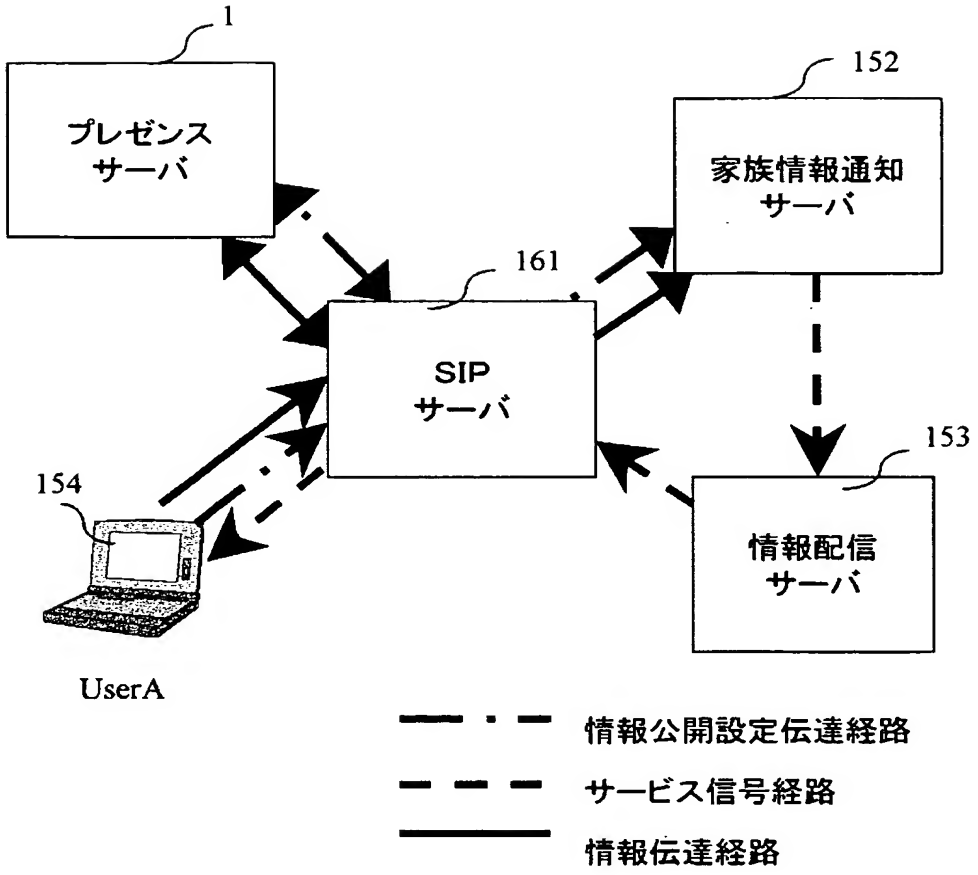
【図１２】

図12


通信事業者
1
プレゼンス
サーバ
サービス提供事業者
152
家族情報通知
サーバ
153
情報配信
サーバ
154
UserA
情報公開設定伝達経路
サービス信号経路
情報伝達経路

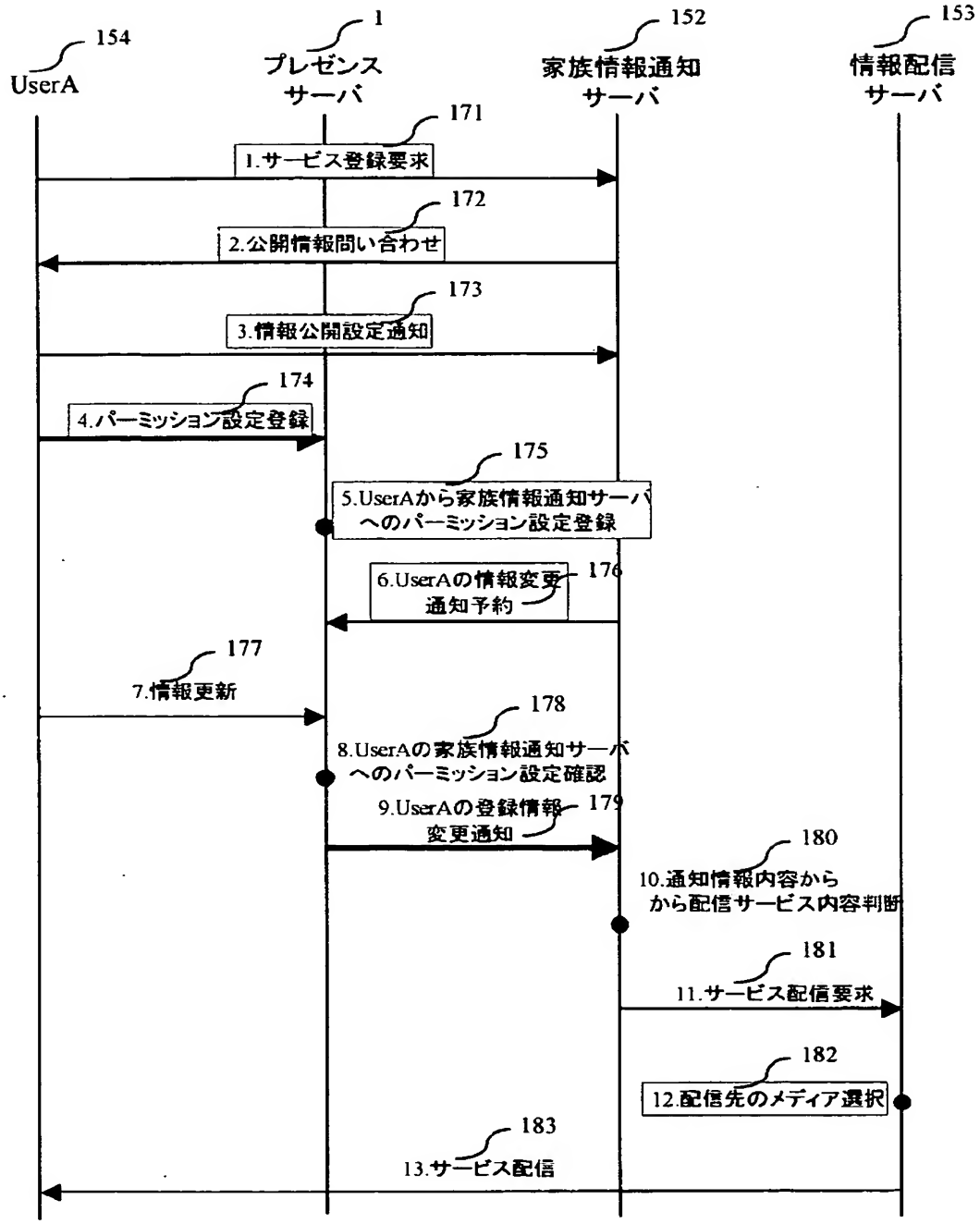
【図１３】

図13


1
プレゼンス
サーバ
152
家族情報通知
サーバ
161
SIP
サーバ
153
情報配信
サーバ
154
UserA
情報公開設定伝達経路
サービス信号経路
情報伝達経路

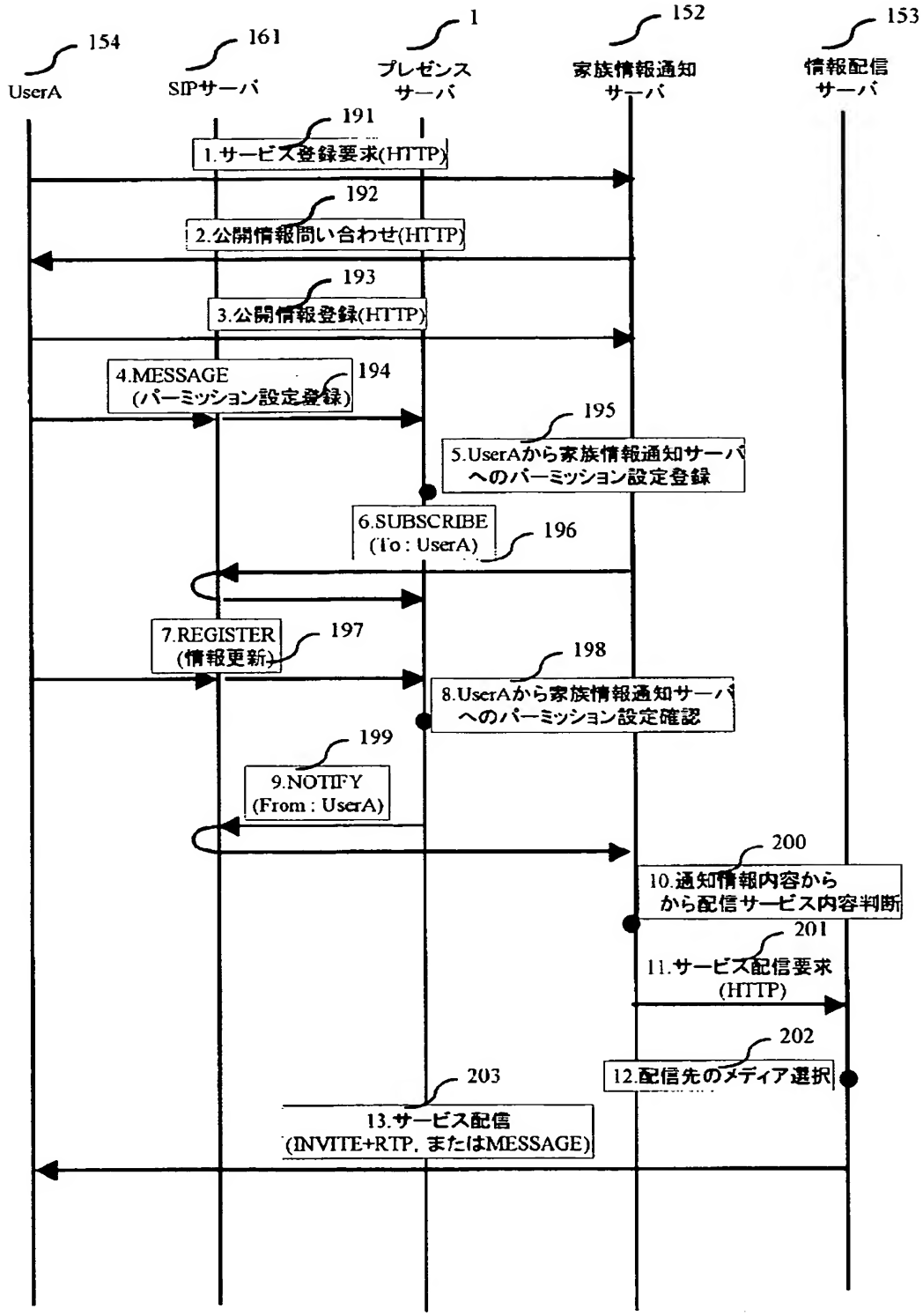
【図１４】

図14


154
UserA
1
プレゼンス
サーバ
152
家族情報通知
サーバ
153
情報配信
サーバ
171
1.サービス登録要求
172
2.公開情報問い合わせ
173
3.情報公開設定通知
174
4.パーミッション設定登録
175
5.UserAから家族情報通知サーバ
へのパーミッション設定登録
6.UserAの情報変更
通知予約
176
177
7.情報更新
178
8.UserAの家族情報通知サーバ
へのパーミッション設定確認
9.UserAの登録情報
変更通知
179
180
10.通知情報内容から
から配信サービス内容判断
181
11.サービス配信要求
182
12.配信先のメディア選択
183
13.サービス配信

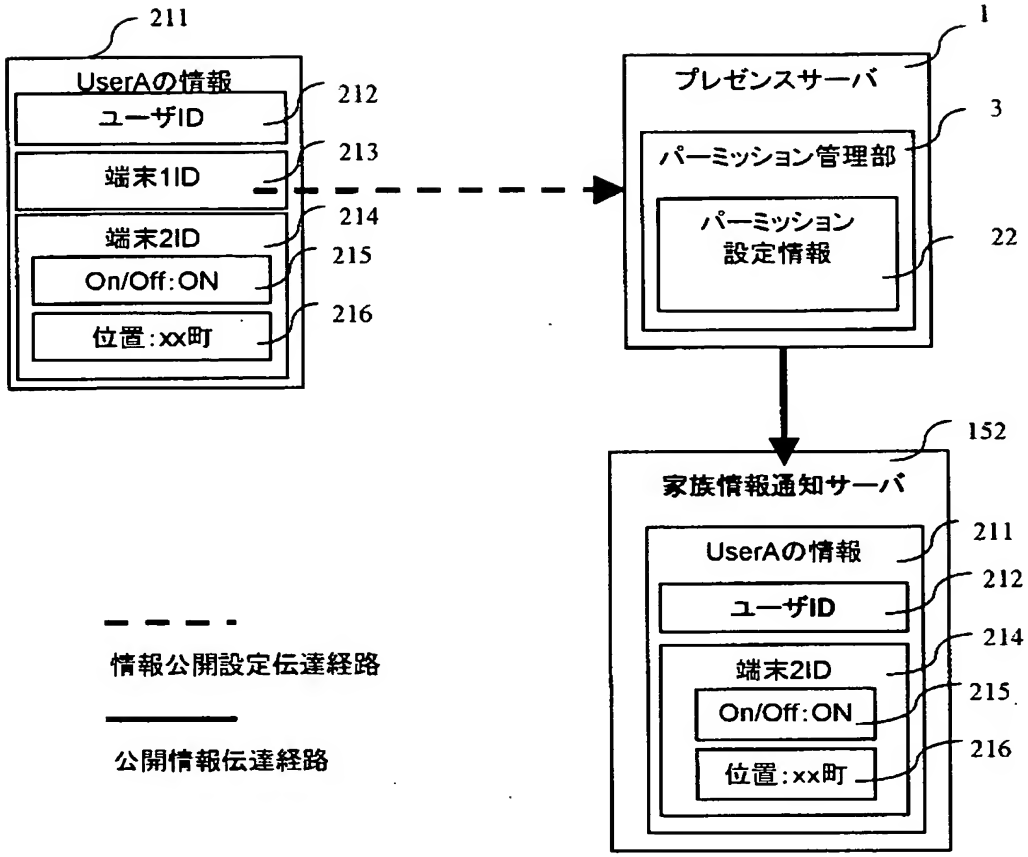
【図１５】

図15


154
UserA
161
SIPサーバ
1
プレゼンス
サーバ
152
家族情報通知
サーバ
153
情報配信
サーバ
191
1.サービス登録要求(HTTP)
192
2.公開情報問い合わせ(HTTP)
193
3.公開情報登録(HTTP)
4.MESSAGE
(パーミッション設定登録)
194
195
5.UserAから家族情報通知サーバ
へのパーミッション設定登録
6.SUBSCRIBE
(To : UserA)
196
7.REGISTER
(情報更新)
197
198
8.UserAから家族情報通知サーバ
へのパーミッション設定確認
199
9.NOTIFY
(From : UserA)
200
10.通知情報内容から
から配信サービス内容判断
201
11.サービス配信要求
(HTTP)
202
12.配信先のメディア選択
203
13.サービス配信
(INVITE+RTP, またはMESSAGE)

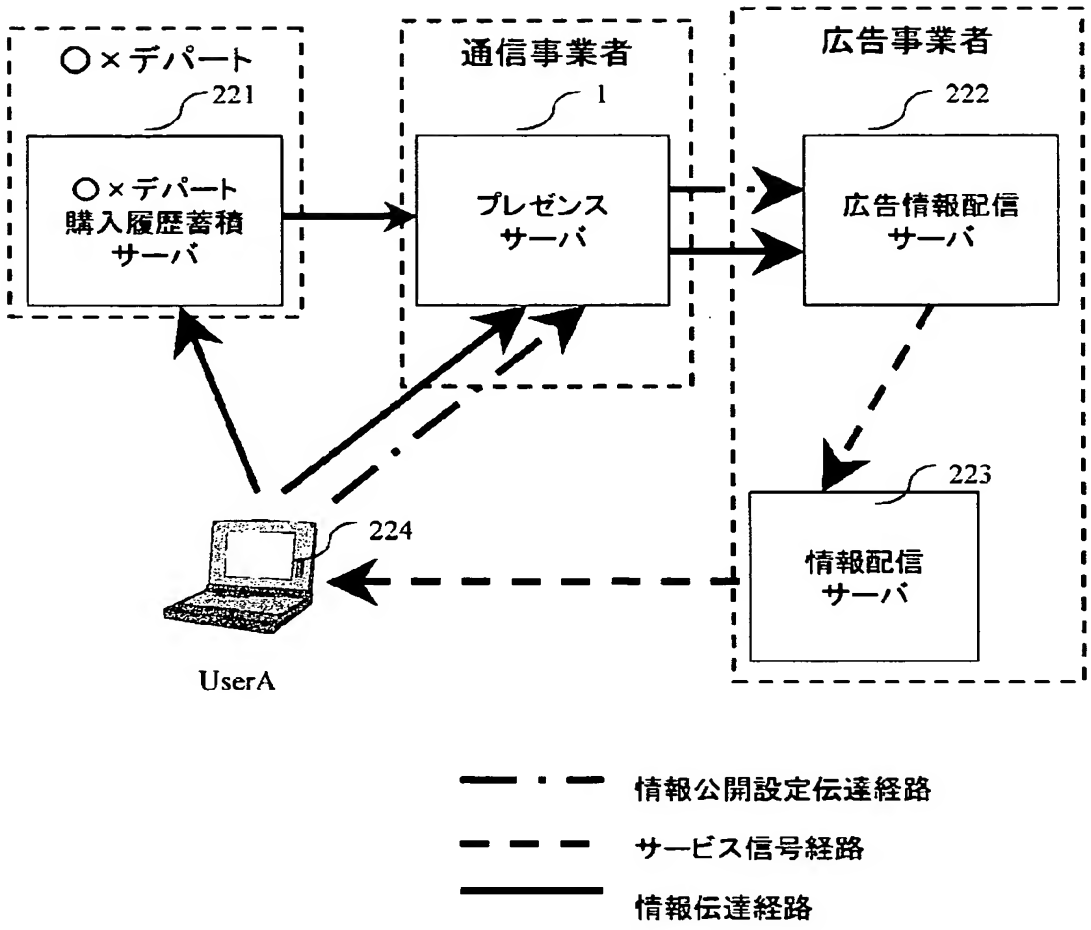
【図１６】

図16


211
UserAの情報
ユーザID
端末1ID
端末2ID
On/Off:ON
位置:xx町
212
213
214
215
216
1
プレゼンスサーバ
3
パーミッション管理部
パーミッション
設定情報
22
152
家族情報通知サーバ
211
UserAの情報
ユーザID
端末2ID
On/Off:ON
位置:xx町
212
214
215
216
情報公開設定伝達経路
公開情報伝達経路

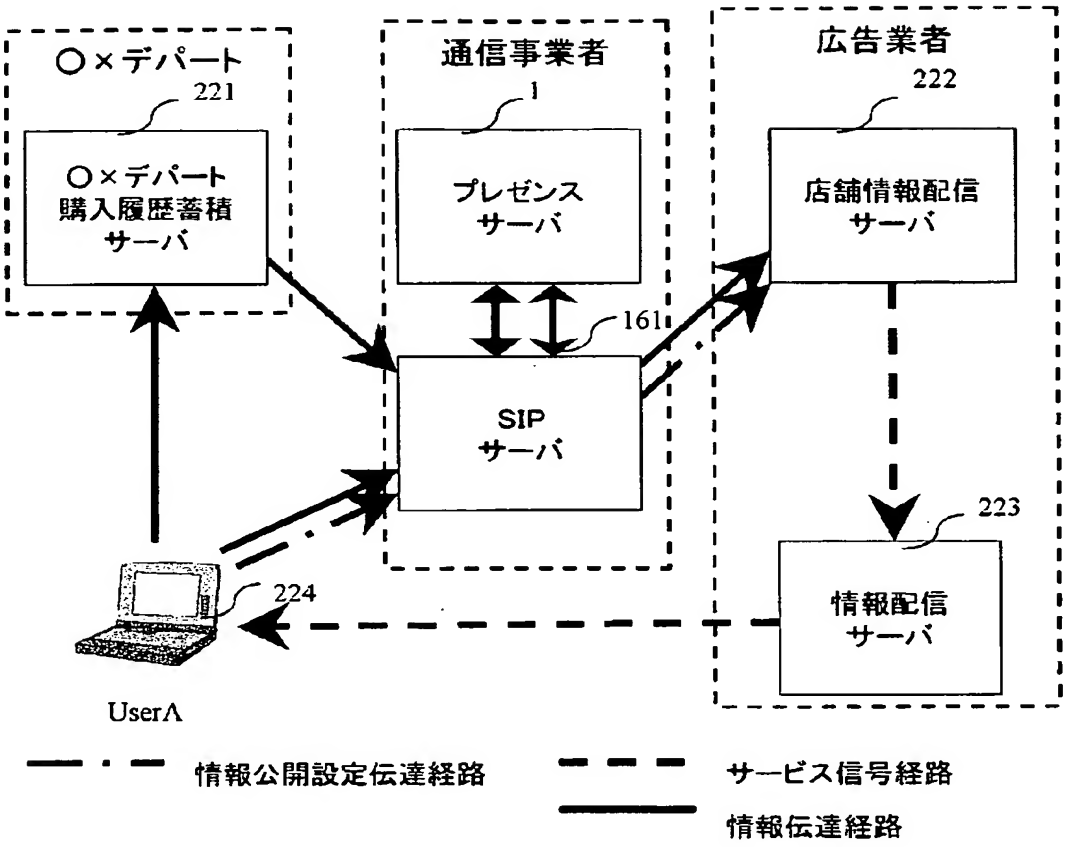
【図１７】

図17


○×デパート
221
○×デパート
購入履歴蓄積
サーバ
通信事業者
1
プレゼンス
サーバ
広告事業者
222
広告情報配信
サーバ
223
情報配信
サーバ
224
UserA
情報公開設定伝達経路
サービス信号経路
情報伝達経路

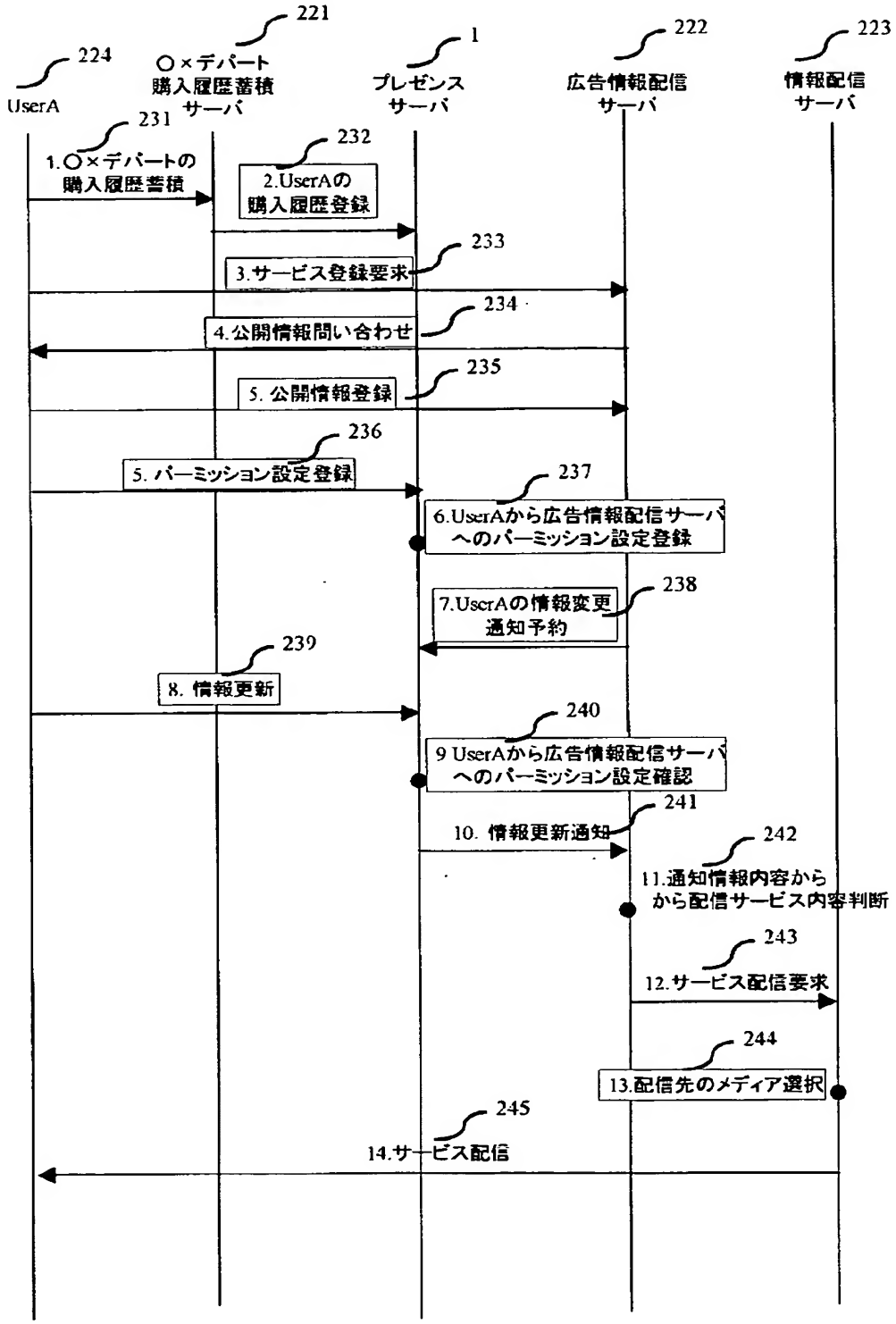
【図１８】

図18


○×デパート
221
○×デパート
購入履歴蓄積
サーバ
通信事業者
1
プレゼンス
サーバ
161
SIP
サーバ
広告業者
222
店舗情報配信
サーバ
223
情報配信
サーバ
224
UserA
情報公開設定伝達経路
サービス信号経路
情報伝達経路

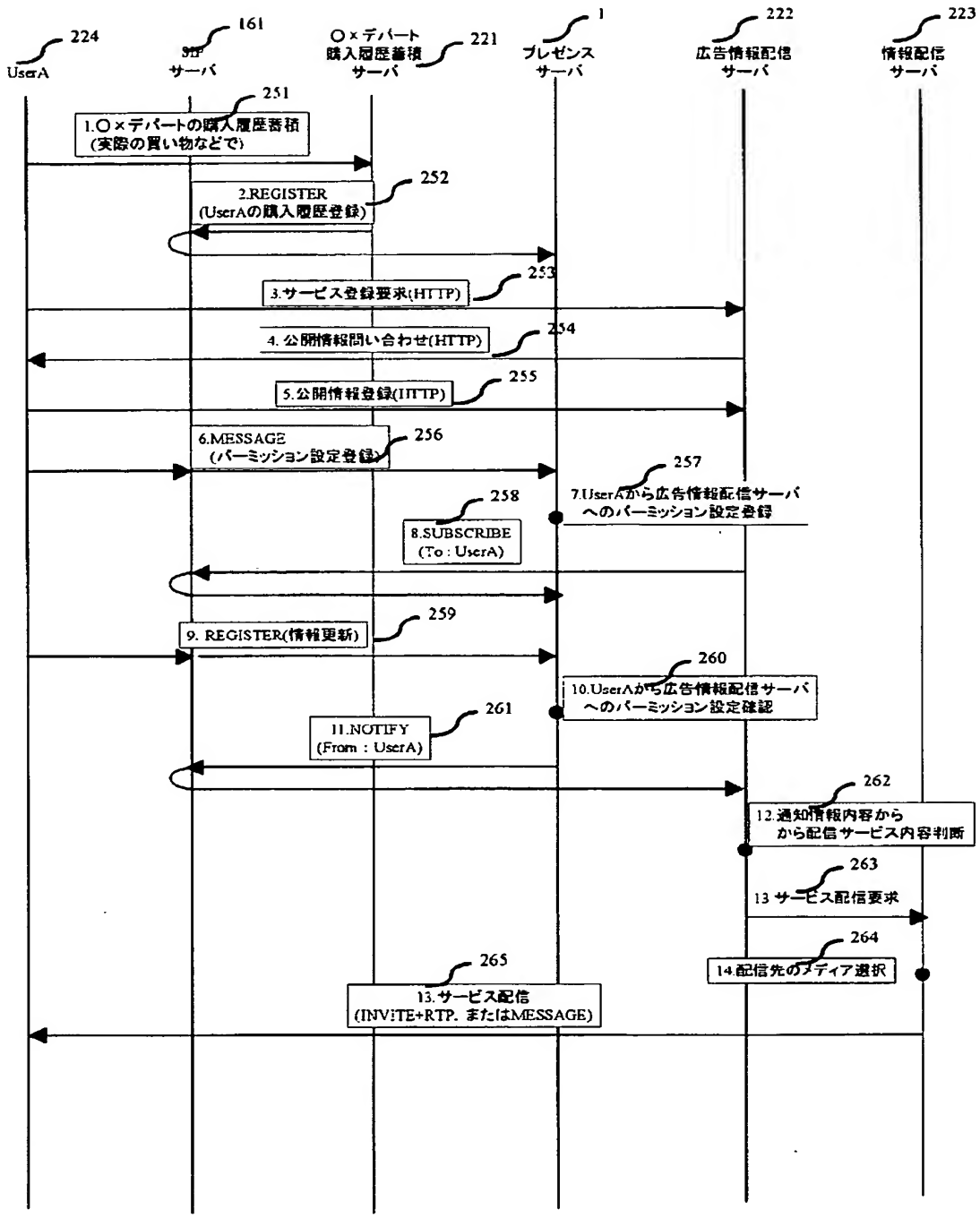
【図１９】

図19


221
224
1
222
223
UserA
○×デパート
購入履歴蓄積
サーバ
プレゼンス
サーバ
広告情報配信
サーバ
情報配信
サーバ
231
1.○×デパートの
購入履歴蓄積
232
2.UserAの
購入履歴登録
233
3.サービス登録要求
234
4.公開情報問い合わせ
235
5. 公開情報登録
236
5. パーミッション設定登録
237
6.UserAから広告情報配信サーバ
へのパーミッション設定登録
238
7.UserAの情報変更
通知予約
239
8. 情報更新
240
9 UserAから広告情報配信サーバ
へのパーミッション設定確認
241
10. 情報更新通知
242
11.通知情報内容から
から配信サービス内容判断
243
12.サービス配信要求
244
13.配信先のメディア選択
245
14.サービス配信

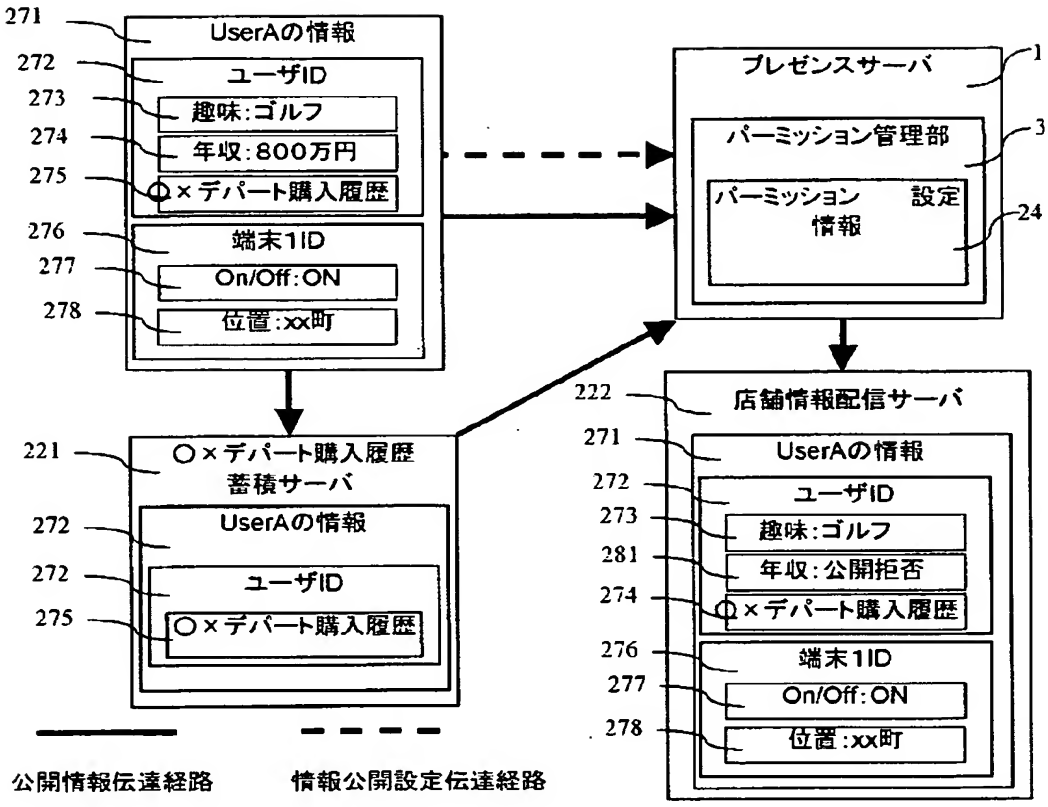
【図２０】

図20


224
UserA
161
SIP
サーバ
○×デパート
購入履歴蓄積
サーバ
221
1
プレゼンス
サーバ
222
広告情報配信
サーバ
223
情報配信
サーバ
251
1.○×デパートの購入履歴蓄積
(実際の買い物などで)
252
2.REGISTER
(UserAの購入履歴登録)
253
3.サービス登録要求(HTTP)
254
4. 公開情報問い合わせ(HTTP)
255
5.公開情報登録(HTTP)
256
6.MESSAGE
(パーミッション設定登録)
257
7.UserAから広告情報配信サーバ
へのパーミッション設定登録
258
8.SUBSCRIBE
(To : UserA)
259
9. REGISTER(情報更新)
260
10.UserAから広告情報配信サーバ
へのパーミッション設定確認
261
11.NOTIFY
(From : UserA)
262
12.通知情報内容から
から配信サービス内容判断
263
13.サービス配信要求
264
14.配信先のメディア選択
265
13.サービス配信
(INVITE+RTP. またはMESSAGE)

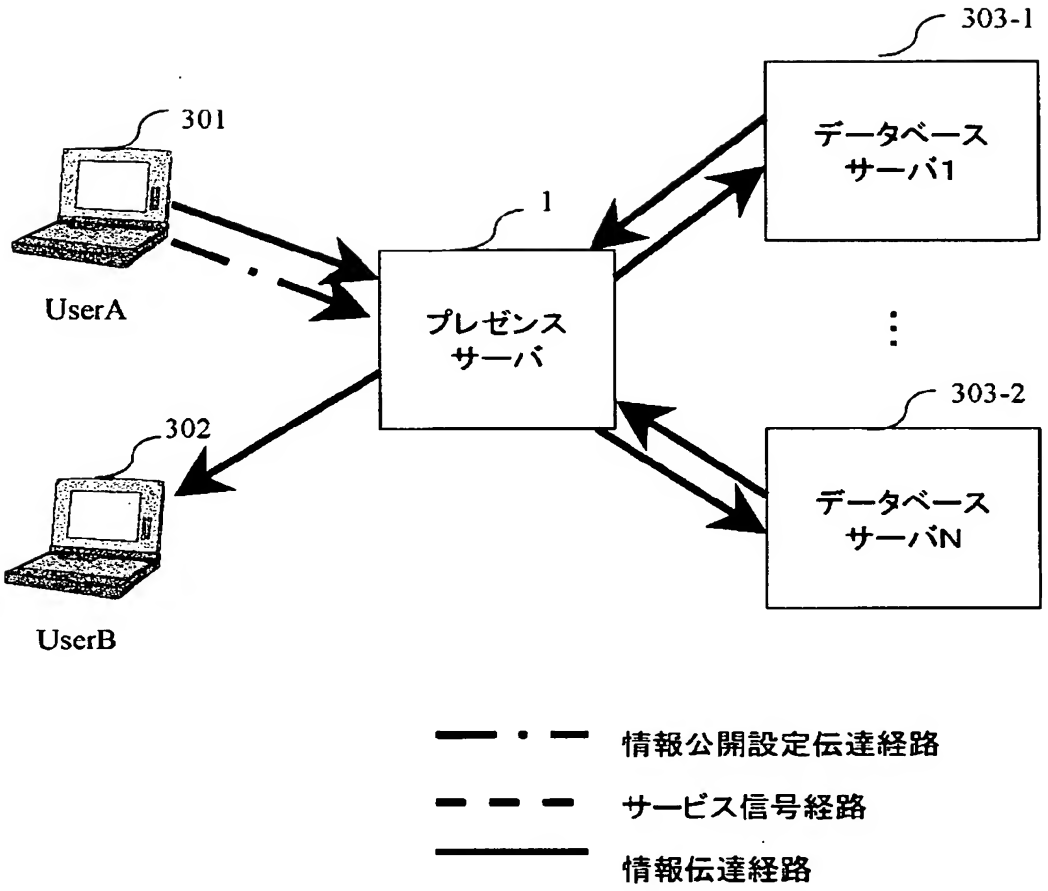
【図２１】

図21


271
UserAの情報
272
ユーザID
273
趣味:ゴルフ
274
年収:800万円
275
○×デパート購入履歴
276
端末1ID
277
On/Off:ON
278
位置:xx町
プレゼンスサーバ
1
パーミッション管理部
3
パーミッション　設定情報
24
222
店舗情報配信サーバ
271
UserAの情報
272
ユーザID
273
趣味:ゴルフ
281
年収:公開拒否
274
○×デパート購入履歴
276
端末1ID
277
On/Off:ON
278
位置:xx町
221
○×デパート購入履歴蓄積サーバ
272
UserAの情報
272
ユーザID
275
○×デパート購入履歴
公開情報伝達経路
情報公開設定伝達経路

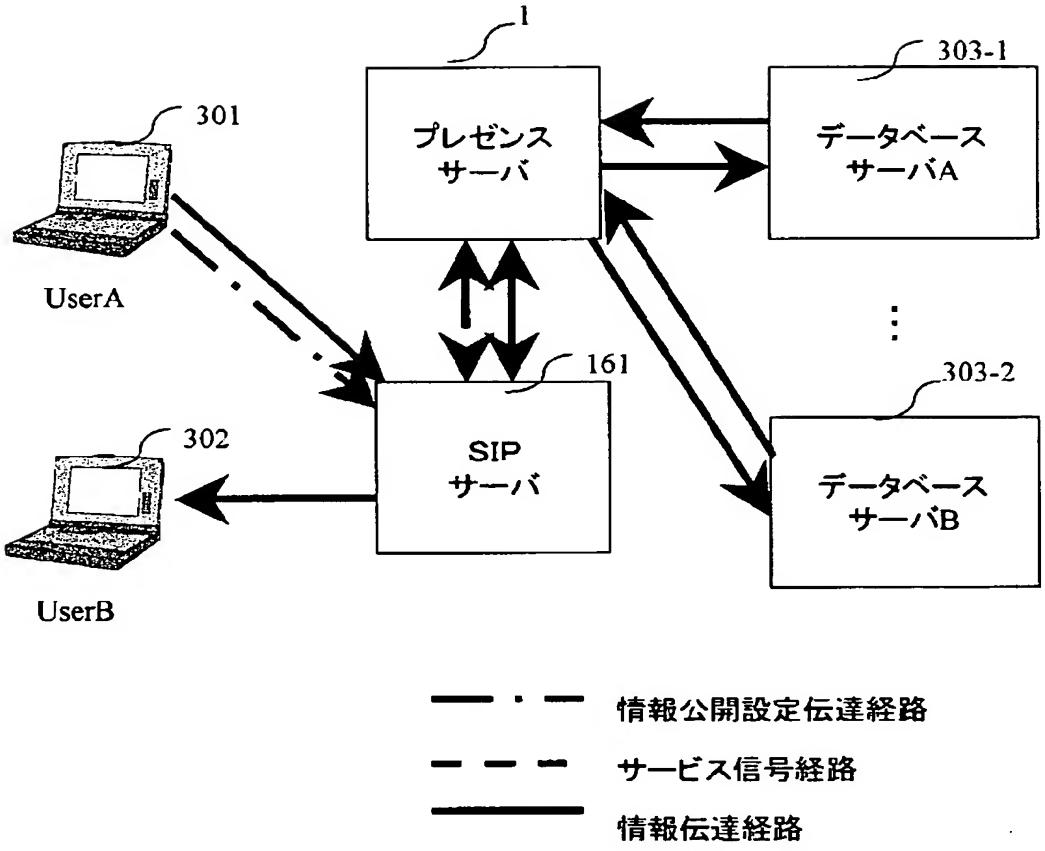
【図２２】

図22


303-1
データベース
サーバ1
301
1
UserA
プレゼンス
サーバ
303-2
302
データベース
サーバN
UserB
情報公開設定伝達経路
サービス信号経路
情報伝達経路

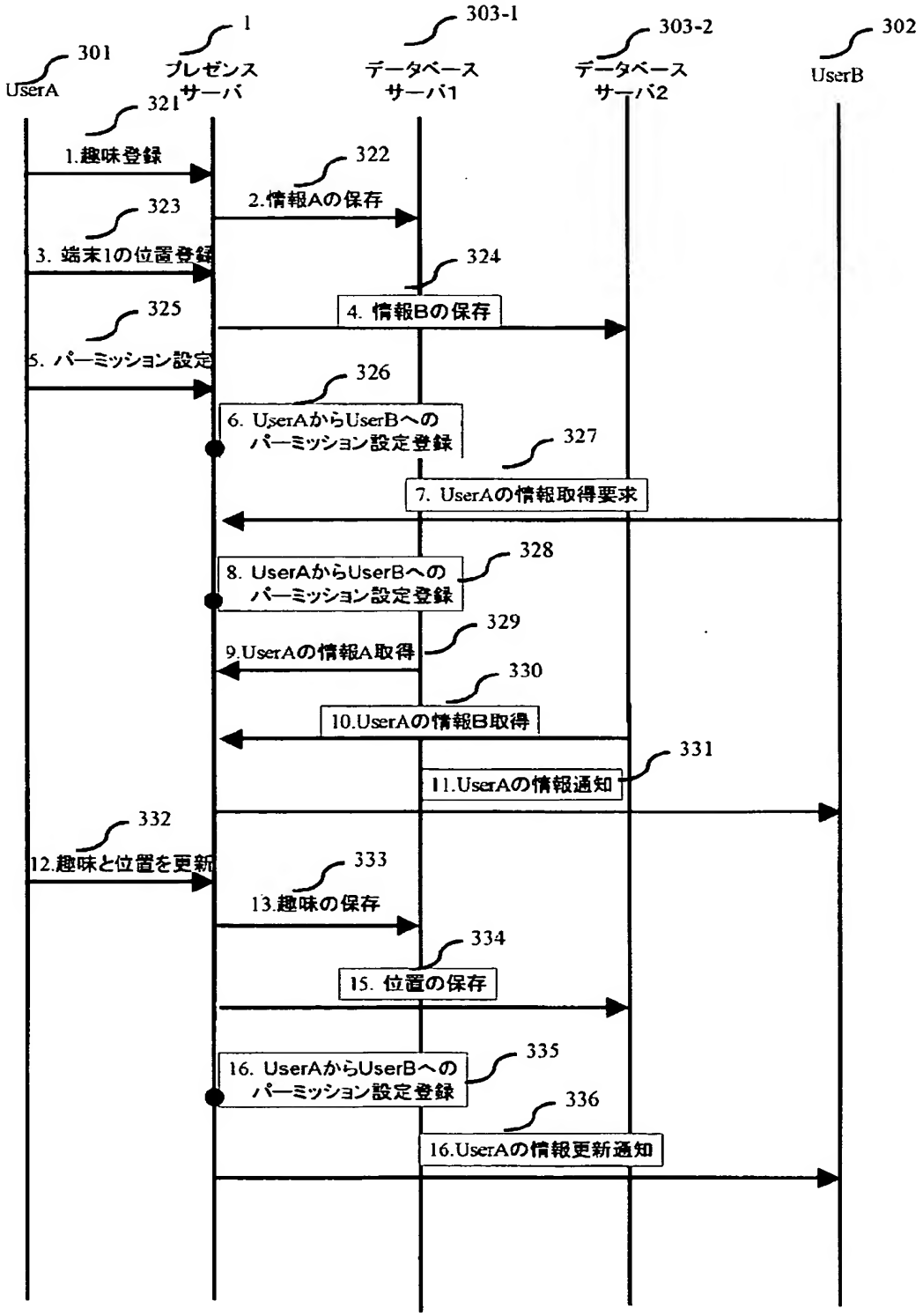
【図２３】

図23


1
303-1
301
プレゼンス
サーバ
データベース
サーバA
UserA
161
303-2
302
SIP
サーバ
データベース
サーバB
UserB
情報公開設定伝達経路
サービス信号経路
情報伝達経路

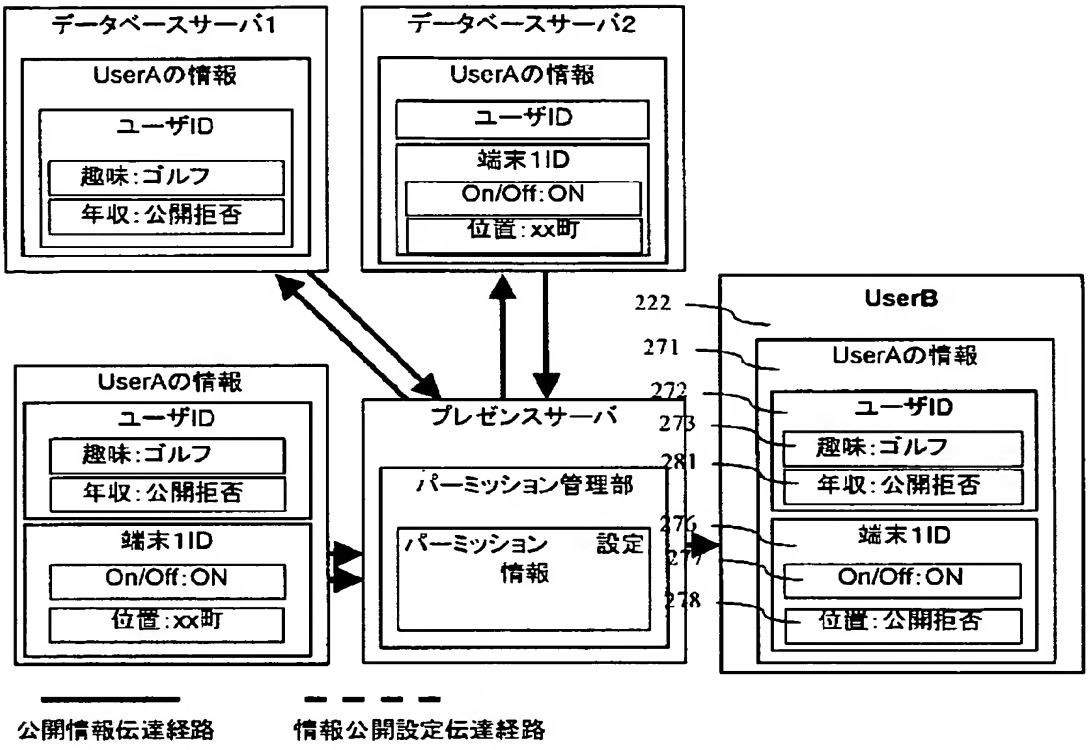
【図２４】

図24


UserA
301
プレゼンス
サーバ
1
データベース
サーバ1
303-1
データベース
サーバ2
303-2
UserB
302
321
1.趣味登録
322
2.情報Aの保存
323
3. 端末1の位置登録
324
4. 情報Bの保存
325
5. パーミッション設定
326
6. UserAからUserBへの
パーミッション設定登録
327
7. UserAの情報取得要求
328
8. UserAからUserBへの
パーミッション設定登録
329
9.UserAの情報A取得
330
10.UserAの情報B取得
331
11.UserAの情報通知
332
12.趣味と位置を更新
333
13.趣味の保存
334
15. 位置の保存
335
16. UserAからUserBへの
パーミッション設定登録
336
16.UserAの情報更新通知

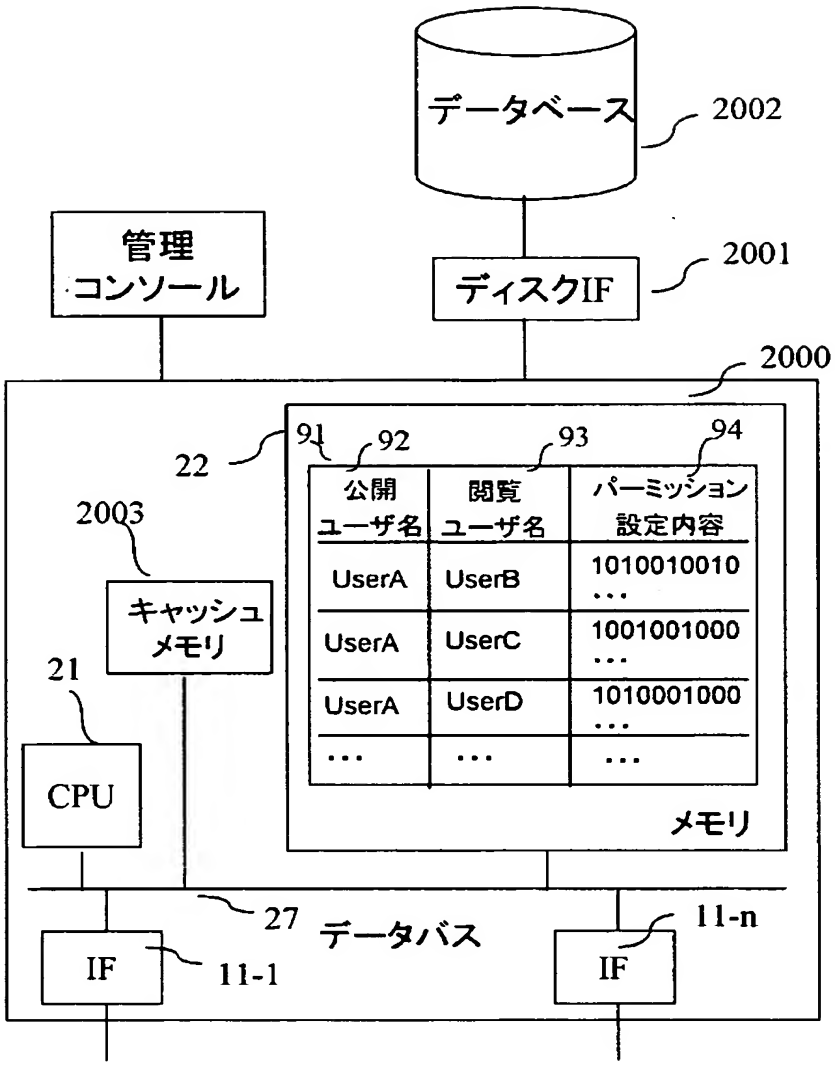
【図２５】

図25


データベースサーバ1
UserAの情報
ユーザID
趣味:ゴルフ
年収:公開拒否
データベースサーバ2
UserAの情報
ユーザID
端末1ID
On/Off:ON
位置:xx町
UserB
222
271
UserAの情報
272
ユーザID
273
趣味:ゴルフ
281
年収:公開拒否
276
端末1ID
277
On/Off:ON
278
位置:公開拒否
UserAの情報
ユーザID
趣味:ゴルフ
年収:公開拒否
端末1ID
On/Off:ON
位置:xx町
プレゼンスサーバ
パーミッション管理部
パーミッション情報
設定
公開情報伝達経路
情報公開設定伝達経路

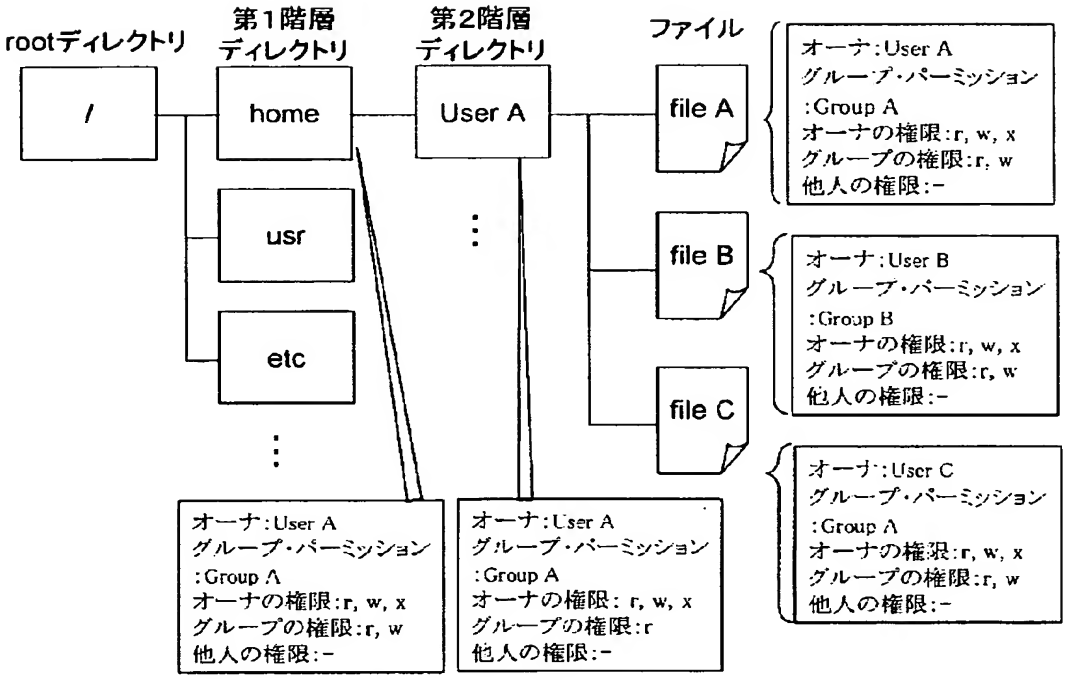
【図２６】

図26


データベース
2002
管理
コンソール
ディスクIF
2001
2000
22
91
92
93
94
公開
ユーザ名
閲覧
ユーザ名
パーミッション
設定内容
UserA
UserB
1010010010
UserA
UserC
1001001000
UserA
UserD
1010001000
2003
キャッシュ
メモリ
21
CPU
メモリ
27
データバス
11-n
IF
11-1
IF

【図２７】

図27



＊グループの構成員
GroupA:UserA,UserC
GroupB:UserA,UserB

＊権限の種別
-：すべて不許可，r :read許可，w：write許可．x：実行許可

【書類名】　　要約書

【要約】

【課題】　個人情報の第三者に対する開示度合いを適切に管理する。

【解決手段】　個人属性情報の開示可否の設定値を、開示レベルに応じて階層的に管理する。また、ユーザが設定値の変更要求を行なった場合、変更される設定値の属する開示可否レベルに応じて、上位下位の設定値の整合性を適切に変更する。

【効果】　設定矛盾の整合によりヒューマンエラーが吸収され、ユーザの個人情報流出に起因するセキュリティの低下を防止できる。また、パーミッション情報を集中管理し、実際にサービスを行なうサーバと分離することにより、個々のサーバの負担が軽減される。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１７７４５６
受付番号	５０３０１０３８０６４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　６月２４日

＜認定情報・付加情報＞

【提出日】　平成15年 6月23日

次頁無

特願２００３－１７７４５６

出願人履歴情報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所